



November 19, 2002

VIA EMAIL

Richard A. Clarke, Chair
Howard A. Schmidt, Vice Chair
President's Critical Infrastructure Protection Board

Re: Draft Strategy to Secure Cyberspace

Dear Messrs. Clarke & Schmidt:

The Securities Industry Association ("SIA")¹ is pleased to offer its comments on the September 2002 draft of The National Strategy to Secure Cyberspace ("Strategy"). The document drafted by the President's Critical Infrastructure Protection Board ("PCIPB") describes initiatives to secure U.S. information systems against deliberate, malicious disruption and to foster an increased national resiliency.

SIA applauds the PCIPB for raising consciousness regarding Internet security and for outlining a strategic response that is intended to be a participatory process rather than a federal government prescription. SIA believes the PCICB outlines appropriately the relative responsibilities of the private and public sectors in securing cyberspace. For example, while government can promote awareness, enable overall communication and coordination, and set minimum expectations, individual industries and entities must have sufficient flexibility to design and implement the specific security strategies that are appropriate for them.

An example of a recommendation in which the level of specificity is a concern for our members is R4-34. This recommendation states that corporations should consider annually disclosing the identity of their Information Technology ("IT") security audit firm and the scope of its work, its corporate and board governance system for IT security, and its adherence to industry best practices. SIA believes that auditing ought to be a

¹ The Securities Industry Association brings together the shared interests of more than 600 securities firms to accomplish common goals. SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. The U.S. securities industry manages the accounts of nearly 93 million investors directly and indirectly through corporate, thrift, and pension plans. In the year 2001, the industry generated \$198 billion in U.S. revenue and \$358 billion in global revenues. Securities firms employ approximately 750,000 individuals in the United States. (More information about SIA is available on its home page: <http://www.sia.com>.)

feature of a corporation's information security planning, but that the issue of who audits and how is a decision best left to individual companies. Moreover, SIA does not believe that full public disclosure of a corporation's policies and procedures relating to information security is necessarily wise. Some of the disclosures may actually compromise information security by publicizing points of vulnerability. It should be sufficient to recommend that firms conduct audits, maintain updated corporate governance policies for IT security and consider industry best practices as part of their IT security planning.

We also support each of the Strategy's guiding principles: private-public partnerships, avoiding regulation, safeguarding civil liberties and privacy, coordinating with Congress, and cooperation with state and local authorities. Together with the recommendations, the document offers a framework for an evolving strategy for securing cyberspace and increasing public awareness.

The broker-dealer community works diligently, both individually and collectively through the Association, on processes and standards to secure its Internet infrastructure and promote business continuity planning generally. SIA is currently working with the Financial Sector Information Sharing and Analysis Centers ("ISAC"), which will permit the Association and its members to receive and disseminate notifications of possible threats and or warnings. SIA agrees that ISAC's such as this one are in the best position to develop strategies for helping to secure the portions of cyberspace that they own or operate.

SIA looks forward to participating in the process envisioned by this document. Please feel free to contact Art Trager, Vice-President & Managing Director, Technology & Operations, SIA (212-618-0546; atrager@sia.com) with any additional questions you may have concerning the views expressed in this letter.

Very truly yours,

Jennifer Bayuk, Chairman
Information Security Subcommittee of the
SIA Technology Management Committee

cc: Information Security Subcommittee
Technology Management Committee
Business Continuity Planning Committee
Technology & Regulation Committee