#43

Securities Industry Association

1401 Eye Street, NW, Washington, DC 20005-2225, (202) 296-9410, Fax (202) 296-9775
info@sia.com, http://www.sia.com

2/18/97

February 13, 1997

Mr. William A. Reinsch
Under Secretary of Commerce
for Export Control
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Avenue, N.W.
Room 2705
Washington, D.C. 20230

Re: Docket No. 960918265-6366-03

Dear Under Secretary Reinsch:

Executive Summary

The Securities Industry Association ("SIA")[1] favors a relaxed export scheme that will facilitate the use of strong encryption products. The proposed changes to the export regulations governing software with encryption capabilities do not satisfy our need to provide strong, secure encryption to protect global business communications. In particular, a lack of attentiveness to liability, accountability, and due process in the Key Management Infrastructure (KMI) make it unworkable as a solution to the export policy problem. Moreover, 56-bit encryption is non-competitive and inadequate for our current and future needs. While the regulation would be an improvement over the current 40-bit limit, well-funded attackers (such as foreign governments) could break 56-bit encryption without much difficulty. The insecurity of the Key Management Infrastructure (KMI) outweighs the benefits offered by providing easier, yet conditional, access to more powerful encryption. We respectfully urge you to consider our comments as you prepare the final regulations.

---

1 The Securities Industry Association is the leading proponent of capital markets, bringing together the shared interests of more than 730 securities firms throughout North America to accomplish common goals. SIA members -- including investment banks, broker-dealers, specialists, and mutual fund companies -- are active in all markets and in all phases of corporate and public finance. In the U.S. SIA members collectively account for approximately 90 percent, or $100 billion, of securities firms' revenues and employ about 350,000 individuals. They manage the accounts of more than 50-million investors directly and tens of millions of investors indirectly through corporate, thrift and pension plans.

120 Broadway, New York, NY 10271-0080, (212) 608-1500, Fax (212) 608-1604

Background

SIA and its Technology Management Committee appreciates this opportunity to express its views on the regulations for encryption products issued by the Bureau of Export Administration on December 30, 1996. At the outset, we want to thank the Administration for its attention to this critical issue. Generally, the regulation establishes new procedures and conditions for companies to follow for gaining approval to export encryption products and creates a new license exception for recoverable encryption products. However, the regulation falls far short of achieving SIA's main priority: to provide strong, secure encryption to protect global business communications with our clients.

Advances in communications technology -- from the network of satellites orbiting the earth to smaller, faster, more user-friendly computers -- have made the world a very small place. The ability to communicate, conduct transactions, and shift funds almost instantaneously with people on the other side of the world has transformed our economy. According to the Department of Commerce, 1990 was the first year capital spending on the information economy -- computers and telecommunications equipment -- exceeded capital spending on all other parts of the nation's infrastructure. Seven years later, our economy is firmly rooted in the digital age.

The U.S. securities industry has capitalized on the opportunities presented by advances in information technology. For the fifth consecutive year, securities firms raised more than a trillion dollars for U.S. business in equity, initial public offerings, corporate bonds, private placements, and domestic medium-term note programs. Figures for the last quarter of 1996 indicate that this trend will continue. The cycle of low interest rates, strong stock prices, a swell of consolidations in various industries, and a favorable economy have been beneficial to investors, issuers, and the industry.

A recent wave of initial public offerings has helped the U.S. securities industry maintain its preeminence in the global economy. In 1996, the industry raised $50 billion for new growth companies, which translates into the creation of hundreds of thousands new jobs. In contrast, no other industrialized country has such a vibrant, entrepreneurial IPO market. In Europe and Japan, where banks play a key role in financing new companies, risk capital is scarce. Few new jobs are created in those economies because competition-limiting regulations effectively shut entrepreneurs out of the capital markets.

In addition to financing the creation of new jobs and economic growth, our industry is also helping Americans prepare financially for their futures. We are the world leaders in international project finance, as we help emerging countries enhance their economic growth. And we are also fueling the technological revolution that is changing the way we live and work. Already, a consumer can sit at her home computer, dial in to her bank, and send checks and buy and sell securities with the click of a mouse. Securities firms and individual companies are underwriting and selling securities over the Internet. Electronic market places for securities are proliferating. Financial services firms more and more are becoming information businesses.

The financial services industry faces serious challenges, in maintaining the security and privacy of customer accounts and information and preventing the opportunity for fraud and other misconduct that could arise as a result of new technology. Security is critical to the securities industry, and for good reason. We have a fiduciary responsibility to our customers and to our shareholders to maintain the confidentiality, integrity and availability of our data. Each year, the industry spends millions of dollars building, buying, implementing and testing the security of its systems and networks.

If we could not maintain the confidentiality of our clients' and our own data, we would lose their confidence and their business. In today's financial environment, we compete with firms from all over the world. The customers we court are investors both within and outside the United States. Our ability to present globally-deployed financial expertise to our clients makes us successful. Indeed, the growth of the Internet and open systems have presented us with new security challenges. As an industry, however, we have no choice but to use the Internet if we are to stay competitive. Our clients want to do business over the Internet and our competitors already do.

Our Requirements

The Wall Street environment is highly competitive. When we have information that gives us a market edge over our competitors, it is crucial that we keep that information secret. When our market analysts spot a trend, it is crucial that we provide that information to our clients -- and only our clients -- without it finding its way into the hands of our competitors. Much of the information in which we trade is extremely valuable. For example, if we are advising a client on a potential acquisition, the name of the target company cannot become public before the client is ready to announce it. Should the information be made public too early, purchases could be made in the market that would make the planned acquisition more expensive, or even impossible to complete.

The financial services industry requires reliable security in its communications between and among its principals, counterparties, and clients, many of who are often non-US companies. The inappropriate disclosure of confidential information could be exploited, causing tremendous financial consequences and undermining the public's confidence in the marketplace. Our industry does not generally have a requirement to escrow communications encryption keys, and we contend that no benefits would result from adding a third party key holder to our communications environment. In fact, such a requirement would introduce several unacceptable security vulnerabilities.

The inadequacy of 56-bit encryption is of particular concern to the securities industry because our firms -- which have access to much of our clients' proprietary data -- are often targeted by foreign governments working on behalf of their domestic industries to gain a leg up on U.S. competitors. It is imperative that we have the tools available to us to ensure the confidentiality of our overseas business communications. While much stronger cryptography is available today from foreign companies -- and many U.S. firms purchase these products overseas to obtain the required security and to avoid U.S. legal

restrictions -- it is difficult to get technical support for foreign products. In addition, the fact that our firms are able to export strong encryption to overseas offices has led some firms to develop different standards for colleagues and clients.

Our Concerns

By placing the key to encrypted messages in the hands of an escrow agent, the KMI introduces a high level of insecurity to the secrecy of communications. Our concern, simply stated, is that the trust placed in these third parties is misplaced. Suggesting that government officials alone will be able to obtain keys from management agents upon a showing of "proper legal authority and without cooperation or knowledge of the user" contains several assumptions that are not logical, especially in a global environment.

We cannot know what "proper legal authority" will mean around the world. Will governments authorize access to confidential business information under the auspices of the need to safeguard national interests that do not pose any real threat to national security? Might governments construe "proper legal authority" to include efforts to keep businesses from moving across borders, directing investments in a manner inconsistent with the government's interests, preserving a tax base, or some other national economic goals? There is strong evidence that certain NATO countries perform industrial espionage on behalf of their domestic industries.[2] Additionally, many non-U.S. governments rely upon legal principles that cannot be expected to offer the same level of protection as a perfectly functioning U.S. legal system. Indeed, Key Holders are heavily beholden to their local government and have little recourse to resolve disputes between themselves and law enforcement, the threat of government pressure becomes very real. Some foreign governments might not even take the pains to allege the appropriate legal authority to gain access to desired keys.

Even without the abuses that could occur under the guise of "proper legal authority," our industry cannot be asked to place its trust in the hands of key management agents located throughout the world, who would be susceptible to compromise from any number of outside influences. Faced with an opportunity to earn significant returns, a corrupt key management agent will thrive. Given the character of the technology, the cause of the damage might never be traceable back to the bad agent. The Administration has even announced plans to introduce legislation limiting the liability of KMI agents. Thus, there will be little practical recourse in the event the confidential information of business parties is compromised by a key agent, whether intentionally or otherwise.

We believe that U.S. industry would be left at a competitive disadvantage if this regulation was implemented in its current form. Current law only allows us to export encryption technologies that use up to 40-bit keys. This rule is certainly an improvement, however, the government itself stated at a meeting with the National Institute of Standards and Technology that well-funded attackers (such as foreign governments)

---

2 See Vol. 139, Congressional Record H2104, (daily ed. April 28, 1993) (statement of Rep. Wolf quoting the *Washington Post*) *CIA: French Targeting Secrets of U.S. Firms -Hughes Cancels Its Exhibit at Paris Air Show.*

could easily break 64-bit encryption. Importantly, many of our clients are already using stronger products that are available abroad and can be imported into the U.S. Those clients would have little incentive to move to a 56-bit key that would provide less protection than is currently available through their foreign suppliers.

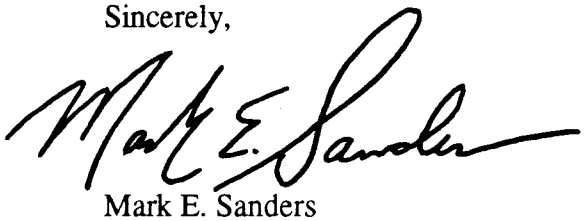
Conclusion

The securities industry is at the forefront of using information and communications technologies to facilitate global business. As more and more of this information is sent electronically, safeguarding the confidentiality of this information has become a vital concern to us. Encryption is the best technology available to us to secure communications between ourselves and our overseas clients and colleagues.

We acknowledge the concerns of the national security and law enforcement communities regarding the widespread use of encryption by those who would threaten national security, and we are prepared to work with them to address these concerns. However, we also note that the charter of these same agencies includes a duty to protect the financial industry from the wrongful use of confidential information by foreign governments and competitors. The proposed export changes improperly sacrifice the needs of the financial services industry for reliable, safe and secure communications.

Thank you for giving us this opportunity to express our views. We look forward to continuing this dialogue with you.

Sincerely,



Mark E. Sanders
Chairman
Securities Industry Association
Technology Management Committee