PREPARED TESTIMONY OF DR. CHARLES W. DENEKA
CHIEF TECHNICAL OFFICER
COMING INCORPORATED
ON BEHALF OF
THE NATIONAL ASSOCIATION OF MANUFACTURERS
BEFORE THE HOUSE JUDICIARY COMMITTEE
ON H.R. 3011, SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT
WEDNESDAY, SEPTEMBER 25, 1996

Thank you and good morning Mr. Chairman. I am Dr. Charles W. Deneka, Senior Vice President and Chief Technical Officer at Coming Incorporated. Also with me today is Dr. James M. Scott - Chief Information Officer & Director of Information Technology for Science & Technology. Established in 1851, Coming Incorporated creates leading- edge technologies for the fastest growing segments of the world's economy. Coming manufactures optical fiber, cable and components, high-performance glass and components for televisions, and other electronic displays for communications and communications-related industries; advanced materials for the scientific, life sciences and environmental markets; and consumer products. Corning's total revenues from continuing operations in 1995 were $3.3 billion. Today, however, I am representing the National Association of Manufacturers and its 14,000 member companies. The NAM supports H.R. 3011, in particular,

the relaxation of unilateral export controls on encryption.The National Academy of Sciences has extensively documented policy change. Thus, my message this morning will be very simple. It is not just computer and communications companies, as suppliers, that suffer serious restrictions from rigid export controls on encryption. And it is not just banks, as users, that need encryption. I am here to say that American industry, in general, needs a relaxation of encryption controls as part of needed relief from onerous unilateral trade policies. Agriculture is often exempted from unilateral trade sanctions; often, airlines as well. In encryption, financial services have been accorded special status. But, time after time, U.S. manufacturers bear the brunt of policies that impose burdens our allies refuse to impose on their firms which are our global competitors.

Think, for a moment, of the new business vocabulary you've recently been hearing: just-in-time delivery; global sourcing; and CAD/CAM (computer-aided design and manufacturing). The new terminology reflects the ways that a business has to operate to be successful now and into the next century: electronically, globally, ever more responsive to customer demands and a shifting business environment. This represents a far different image of manufacturing success than what we all learned in school,

when we saw pictures of Henry Ford's assembly line of identical Model T's destined for a domestic market.

Let me give you an example from my own company, Coming Incorporated. Coming is a technology company which has a long and rich history of "inventions," secrets upon which the future of the company depends. This information must not be accessed by potential competitors, either in the private or government sector. We have a major laboratory in France and a smaller, but important lab, in Japan that we are concerned about communicating with. It is our opinion that, unlike financial information, whereinformation may have little commercial value minutes or hours after it has been intercepted, the information that we need to share across our global facilities has a useful "lifetime" of years, if not decades. Unless robust encryption technology is available, a potential competitor could decrypt information about our inventions at their leisure. This would cause us great harm.

The future of Coming depends upon new products spawned by our world- wide research and development facilities. Our innovation process depends upon the ready access of proprietary information by research associates in our facilities around the globe. In order to make progress, the information must be accessed by authorized personnel in a secure manner, with no possibility of this information leaking out until the appropriate patent or commercial action has been taken. We, therefore, feel that to protect our intellectual capital from penetration by foreign competition or government bodies, the encryption technology deployed must be sufficient to prevent this, even when there is no time limit on decryption efforts.

Types of highly proprietary information that Coming associates need to access on a world-wide basis includes:

- Research Reports

- Patent Information Process Information

- Product Plans Market Plans

An alternative to secure, encrypted communications and systems may appear to be for Coming employees or couriers to physically go to the non-U.S. labs and carry with themeither paper copies or laptop computers. The major problems with this approach which prevent it from being viable are:

- Only a limited number of our people can travel because of the high cost, and while they are traveling they are out of their labs so they cannot be productive in advancing technology further.

The time lag created by moving paper physically by any means would be intolerable in this world of rapidly increasing rate of change. It would be like going back to the Pony Express days.

Finally, our people have very frequent, often dally, communications. During critical phases of projects we often have real-time discussions involving many people on each side. In addition to needing secure communications between Corning's own U.S. and international labs, we also absolutely need to have this security when dealing with other non-U.S. companies. We have had, and will continue to have, highly sensitive and very important joint research and development programs with suppliers of specific raw materials, some of which are crucial to the performance of our products, as well as with existing and potential new customers. We also do research and development with some universities and government laboratories when it helps us develop or improve our products. This is a natural consequence of the global flow of materials and knowledge back and forth across national boundaries through the value chain often seen in medium and high-tech products of today. These communications must be protected.

We are concerned about our ability to do business in a global marketplace, taking advantage of innovation abilities in other countries, unless we have sufficient safeguards on our know-how, inventions, processes, product and market plans.

The successful manufacturer of the future will be an "agile enterprise," to use the phrase pioneered by another auto leader, Lee Iacocca. Production runs will get shorter and shorter, even down to production lots of one. Long-term, intimate, supplier-customer relationships will manage joint design and development of components and will assure just-in-time deliveries. In this environment, protecting only electronic funds transfer cannot and will not suffice. Valuable proprietary data designs, tests and customer lists will flow electronically and must be protected as well. Already in the United States, the one-third ofthe economy outside of manufacturing supports the one-fifth of the total economy that comprises direct

manufacturing. And, as you well know, business has gone global forever.

All these developments explain why the current export controls will have to give way sooner or later.

Fundamentally, they are incompatible with the way that successful, agile enterprises, especially manufacturers, have to function now and into the 21st-century global economy. It is only a matter of when the unilateral controls will be relaxed, and how much damage U.S. business suffers in the meantime compared with foreign competitors not equally burdened.

Even before encryption emerged as a key functional specification, major corporations had already evolved complicated, sophisticated, data communications systems to manage worldwide operations, meet customer demands, and gain competitive advantage. Many of these stories are now part of business history that everybody knows. American Airlines pioneered computer-based reservations almost three decades ago. The market-leading innovations of Federal Express in the package delivery market now includes a much used World Wide Website. For manufacturing, the innovations are less evident from the end- consumer point of view, but are led by the major manufacturers. For example, in communicating with their supplier base, Boeing deals with almost 50,000 contractors and subcontractors through its tightly managed computer network. General Motors led the way in electronic data interchange (EDI) by insisting that its suppliers work with it to get rid of tons of paperwork.

Security is simply an indispensable element of system performance, like processing capacity or uptime. Logical protection against outside intrusion, which is what encryption is all about, is an indispensable element of security.

The very limited export licenses now granted do not provide sufficient security. Weneed secure global connectivity with our foreign suppliers and customers, not just our subsidiaries. In the long run, we cannot win in global competition without that security. If we cannot offer the requisite security, then our suppliers and customers will do business with other companies that can.

A topic that must not go unnoticed this morning is industrial espionage. The FBI has testified before Congress that agents of 23 foreign countries are targeting U.S. enterprises to steal their best technology. The NAM agrees that the threat is real and that losses have occurred. The FBI's answer is a new federal statute with very strong penalties, the better to prosecute technology theft.

Mr. Chairman, the irony is overwhelming. Even as the FBI seeks heavy after-the-fact penalties for people who get caught, they oppose this legislation to put better means of prevention in the hands of the targets and victims: U.S. companies. The government contradicts itself, the NAM submits, in claiming that industrial espionage carried out with the power of foreign intelligence is a big problem, while simultaneously stopping industry from deploying the self-protective measures that it seeks. An ounce of prevention is worth a pound of cure. The FBI simply cannot have it both ways. Once information falls into the wrong hands, there is no way to get it back. American manufacturers need to prevent this from happening in the first place.

Mr. Chairman, this concludes my statement and I will be happy to take questions.