Statement of Mr. Bob Weaver

Deputy Special Agent in Charge
New York Field Office
United States Secret Service

Before

The House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
and the Subcommittee on Oversight and Investigations

U.S. House of Representatives

April 3, 2003

Chairman Bachus, Chairwoman Kelly, Congressman Sanders, Congressman Gutierrez and members of both subcommittees, I appreciate the opportunity to participate in this important hearing.

I look forward to discussing with you today the successes of the Secret Service's New York Electronic Crimes Task Force (NYECTF), and the contributions we have made to the prevention of technology-based crimes, and the protection of our financial and critical infrastructures. I believe we have made a real difference in the effort to strengthen our economic security.

Task forces, in general, are not a new concept to law enforcement, and have been with us for some time. What makes the NYECTF so unique is the diversity of our membership and the personal, trusted relationships that develop between our members. Today, the task force consists of over 250 individual members representing federal, state and local law enforcement, the private sector, and academia. Our members include the largest financial services, telecommunications, and technology companies in the country. It also includes computer science specialists from 18 different universities. Among these partners, most of whom are strong competitors in the consumer marketplace, there is an unprecedented sharing of expertise, information and proven solutions, all of which have been employed in our common mission to prevent the disabling or compromise of critical systems and infrastructure.

Since 1995, the New York task force has charged over 1,000 individuals with electronic crime losses exceeding $1.0 billion. It has trained over 60,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. The task force has identified tools and methodologies that can be employed by our partners to eliminate potential threats to their

information systems. We consider the NYECTF to be the 21st century law enforcement model that modernizes criminal justice and incorporates partnerships and information sharing within its core competencies. The NYECTF applies a systematic approach of protection, preparedness, detection and prevention directed at electronic crime.

This approach has been implemented successfully in various venues around the country. Pursuant to the Public Law 107-56, the USA/PATRIOT Act of 2001, the Secret Service has established Electronic Crimes Task Forces (ECTFs), based on our New York model, in Boston, Miami, Charlotte, Chicago, Las Vegas, San Francisco, Los Angeles, and Washington, D.C. These task forces are applying the blueprint and the methodologies of the NYECTF to develop partnerships and programs that are best suited to the needs of their individual communities. We never lose sight that one of the central tenets of the Secret Service's historic investigative mission is to serve the communities we protect.

The systemic approach of the task force is based on a business model. Its methodology incorporates the principles of preparedness, prevention, detection, response, education, training and awareness, pre-incident response risk management, investigations, and prosecution. This holistic approach combines a business strategy with a cultural change, producing a unique "teamwork" concept targeting risk management, crisis management, disaster recovery, best practices, due diligence, pre-incident response planning, and enterprise protection planning.

The NYECTF is a government success story, highlighted by an unparalleled sharing of information, a unique ability to analyze data with a diversity of partners, and a community-centered civil defense focus for the protection of our national security.

I believe what separates and distinguishes this task force from all others is our commitment to building trusted partnerships and placing the highest priority on that which is in the best interests of the community. Our commitment and contribution to the community is the greatest strength of the New York task force. Our core mission has always been simple -- to make a difference, to have an impact on the community, and to respond to the needs of our law enforcement partners, consumers, and private industry. The community has always been and always will be our focus.

On September 11, 2001, the Secret Service lost its New York Field Office in the collapse of 7 World Trade Center. Our office was destroyed and most of our criminal records, equipment and even personal effects were lost. But it was the community that we serve that stepped in almost immediately to help us rebuild.

I cannot tell you how proud I am of not only the men and women of the Secret Service who work tirelessly on the task force day and night but also the assistance and support of our task force partners – support that can never be quantified. As a result of their support, the New York task force became operational within 48 hours of the terrorist attack and immediately began fighting back.

The most compelling testimony to the expertise and success of the NYECTF is the large number of regular requests received from local and foreign law enforcement agencies for either training or consultation in support of their own initiatives and programs.

These requests have come from agencies nationwide, as well as foreign countries such as Australia, Bulgaria, Canada, England, Ireland, India, Italy, Japan, the Philippines, and Thailand. The Secret Service recognizes the need to promote international cooperation and remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, regarding program initiatives and current telecommunications, financial and electronic crime trends. We are committed to working closely with our foreign law enforcement counterparts in response to cyber crime threats to commerce and financial payment systems. We currently have 18 overseas field offices and a permanent assignment at Interpol, as well as several other international initiatives. Our foreign presence increases our ability to become involved in foreign investigations that are of significant strategic interest to the United States.

As a footnote, the New York task force meets regularly with representatives from Wall Street, The Clearing House, Financial Services Round Table, Security Industry Association, Financial Services Sector Coordinating Council, Treasury Department, and the Financial Services Information Sharing and Analysis Center (FS/ISAC). The role of the FS/ISAC is to facilitate the sharing of information related to cyber threats and vulnerabilities within the financial services industry. The Secret Service is exploring common areas of interest with the FS/ISAC, including information sharing and information technology, as well as expertise in technical and physical security.

Over the last two decades, the U.S. financial services industry has benefited greatly by advances in e-commerce and telecommunications. The same technological developments that have so significantly contributed to the financial services industry's growth and importance, however, have also provided increased opportunities for electronic crime. Our task force recently hosted the New York Financial Services Industry Interactive Exercises for Critical Infrastructure Preparedness. These exercises are commonly referred to as "table top" exercises and are designed to address critical infrastructure security issues facing financial institutions. They facilitate interaction and communication on these issues among senior financial executives, financial industry trade associations, subject matter experts, academia and government officials.

These exercises will build upon the development of a new trusted relationship between the government and the private sector. Just like our task force, the table top exercises will foster personal interactions, networking opportunities, and give all who participate valuable information as well as avenues for resolution to future potential problems.

In today's high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration among the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that

building trusted partnerships with the private sector and local law enforcement is the model for combating electronic crimes in the Information Age.

That concludes my prepared statement, and I would be happy to answer any questions that any of the members of the two subcommittees may have.