Statement of Mr. Timothy Caddigan

Special Agent in Charge - Financial Crimes Division
U.S. 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, thank you for inviting me to be part of this distinguished panel, and the opportunity to address the committee regarding the Secret Service's efforts to combat cyber crime and protect our nation's financial and critical infrastructures.

Let me also take this opportunity to thank Chairman Oxley, Congressman Frank and all members of the full committee for their longstanding support of the Secret Service and the interest this committee has conveyed in our mission, our programs and our employees.

As you know, the Secret Service was created just after the conclusion of the Civil War to address the burgeoning problem of counterfeit currency. At that time, it was estimated that approximately one-third of all currency in circulation was counterfeit, and the government recognized the urgent need to address this issue in order to maintain the public's confidence in our currency. In effect, the Secret Service was engaged in an effort to protect a vital governmental function long before any notion of critical infrastructure protection had emerged.

Today, the Secret Service continues to suppress counterfeit currency as part of its traditional role but also now includes fighting cyber crime as part of our core mission to safeguard the integrity of this nation's financial payment systems. Over time, modes and methods of payment have evolved and so has our investigative mission. Computers and other "chip" devices are now the facilitators of criminal activity or the target of such. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals -- all of whom recognize new opportunities and employ anonymous methods to expand and diversify their criminal portfolio.

In this era of change, one constant that remains is our close working relationship with the banking and financial sectors. We developed this history of cooperation with the industry as a result of our unique responsibilities as a law enforcement bureau of the Department of the Treasury for the last 137 years. Even as a part of the new Department of Homeland Security, those relationships continue to grow and prosper as we continue to work with the Department of the Treasury and the financial sector to protect the banking and financial infrastructure.

Mr. Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial sectors and the need to create effective solutions. There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment. This is where the Secret Service can make a significant contribution to the discussion of successful law enforcement efforts to combat cyber crime -- efforts that are central to the mission of critical infrastructure protection.

The concept of task forces has been around for many years and these groups have been employed at many levels within the law enforcement community. However, traditional task forces have consisted primarily of law enforcement personnel to the exclusion of other parties who could make significant contributions. The New York Electronic Crimes Task Force developed a new approach which enabled local, state, and federal law enforcement officials to collaborate with prosecutors, private industry and academia to fully maximize what each has to offer in furtherance of a common goal -- the protection of America's financial infrastructure.

The Secret Service applied this new approach to our own investigate mission and developed a highly effective formula for combating high tech crime, a formula that has been successfully implemented by the New York Electronic Crimes Task Force (NYECTF). While the Secret Service leads this innovative effort, we do not control or dominate the participants or the investigative agenda of the task force. Rather, the task force provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

Arrests have traditionally been the ultimate goal of law enforcement investigations, but we believe there must be additional means that are just as effective, if not more effective, in the battle against cyber criminals. As such, the new Electronic Crimes Task Force (ECTF) model stresses prevention through partnership. We focus on the mitigation of damage and the quick repair of any damage or disruption to get the system operational as soon as possible after an intrusion occurs. This approach requires the detailed planning and preparation that comes from the relationships, partnerships and level of trust that

have been developed through the ECTFs between law enforcement, academia and the private sector.

The NYECTF, established in 1995, has brought together 50 different federal, state and local law enforcement agencies as well as prosecutors, academic leaders and over 100 different private sector corporations. The wealth of expertise and resources that reside in this task force coupled with unprecedented information sharing yields a highly mobile and responsive machine. In task force investigations, local law enforcement officers hold supervisory positions and representatives from other agencies regularly assume the role of lead investigator. These investigations encompass a wide range of computer-based criminal activity, involving e-commerce frauds, intellectual property violations, identity crimes, telecommunications fraud, and a wide variety of computer intrusion crimes that affect a variety of infrastructures.

Pursuant to Public Law 107-56, the USA/PATRIOT Act of 2001, the Secret Service was authorized to establish a nationwide network of ECTFs, based on our New York model. Subsequently, we have organized task forces in Boston, Charlotte, Chicago, Los Angeles, Miami, San Francisco, Washington D.C., and Las Vegas. These locations were selected based on the presence and support of financial, information technology and government entities; the perceived need for such a task force in that area; the incidence of hi-tech criminal activity; and our interest in a balanced geographic distribution across the country.

An important component in our investigative response to cyber crime is the Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training in the forensic identification, preservation, and retrieval of electronically stored evidence. Special Agents entering the program receive advanced training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers, personal data assistants, telecommunications devices, electronic organizers, scanners and other electronic paraphernalia.

Since 2000, our ECSAP agents have completed over 3,463 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams performed for other law enforcement agencies during this period, it is estimated that some 10 to 15 percent of these examinations fell in this category. Many of the examinations were conducted in support of other agencies' investigations, such as those involving child pornography or homicide cases, simply because the requesting agency did not have the resources to complete the examination itself.

We provide physical assistance on a regular basis to other departments, often dispatching ECSAP agents overnight to the requesting venue to perform computer-related analyses or technical consultation. In fact, so critical was the need for even basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to

Searching and Seizing Electronic Evidence" which is designed for the first responder, line officer and detective alike.

We have also worked with these same partners in producing the interactive, computer-based training program known as "*Forward Edge*," which takes the next step in training officers to conduct electronic crime investigations. *Forward Edge* is a CD-ROM that incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the training program and are immediately accessible for instant implementation.

Thus far, we have dispensed over 300,000 "Best Practices Guides" to local and federal law enforcement officers and have distributed, free of charge, over 20,000 *Forward Edge* training CDs.

Let me relate the Secret Service's mission in fighting cyber crime to the bigger picture of critical infrastructure protection and partnerships. We target electronic crime as it may affect the integrity of our nation's financial payment and banking systems, one of our most important critical infrastructures. Yet our efforts to combat cyber attacks, which target the information and communications systems that support the financial sector, are part of a more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected. Moreover, the public's confidence is lost if such delivery systems and services are unreliable or unpredictable, regardless of the cause of the problem.

The Secret Service has focused its efforts with regard to information security within a relatively narrow spectrum defined by its jurisdictional authorities and our financial payment systems. In this respect the Secret Service ECTF initiative has played, and will continue to play, an increasingly critical role.

The Critical Systems Protection Initiative (CSPI), a collaborative effort between the Secret Service and Carnegie-Mellon University, is working to establish standards, guidelines and methodologies to incorporate a "cyber security" component to our vital mission of protecting our highest elected leaders and events of national significance. This initiative is truly groundbreaking in that it considers both the physical vulnerabilities of a venue for security requirements as well as a "fourth dimension" -- the supporting information technology infrastructure. We recognize that a well-executed cyber attack against a weak technology or support infrastructure system can render an otherwise sound physical security plan vulnerable and inadequate.

A prime example of this was the implementation of both physical and cyber security plans at the 2002 Winter Olympics in Salt Lake City, Utah. The 2002 Winter Games represented the largest coordinated effort in American law enforcement history, and as part of this effort a number of our agents and specialists were specifically assigned to the

task of preventing, investigating and managing numerous intrusion attempts and email threats. These same principles and practices, updated as they adjust to advances in technology, will be implemented during future national events, such as the 2004 Democratic and Republican National Conventions.

It should also be noted that all deliberate infrastructure attacks are also cyber crimes and are likely to be first addressed by law enforcement personnel, both federal and local, in the course of routine business. In fact, there does not appear to be any sort of universal agreement as to when a "hack" or network intrusion rises to the threshold of an infrastructure attack, but we would all probably recognize one when it reached catastrophic proportions.

Given this interplay between computer-based crimes and national security issues, the investigation of electronic attacks against the financial sector is a significant component of larger plans for the protection of our nation's critical infrastructures. When we arrest a criminal who has breached and disrupted a sensitive communications network and are able to restore the normal operation of the host -- be it a bank, telecommunications carrier, or medical service provider -- we believe we have made a significant contribution towards assuring the reliability of the critical systems that the public relies upon on a daily basis.

The Secret Service believes there is value in sharing information during the course of our investigations with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. When sharing such information, the Secret Service takes appropriate steps to protect privacy concerns and ensure that there are no conflicts with prosecutorial issues. I would add that there are many opportunities for the law enforcement community to share information with our private sector counterparts without fear of compromise. The Secret Service recognizes the need for a "paradigm shift" with respect to this type of information sharing between law enforcement and our private sector and academic counterparts.

Law enforcement in general is not sufficiently equipped to train the masses nor can it compete with academic institutions of higher learning in the area of research and development. However, our partnerships with industry and academia have demonstrated that this can be an integral part of the solution. Partnerships are a very popular term in both government and the private industry these days and everyone agrees that there is great utility in such an approach. Unfortunately, however, partnerships cannot be legislated, regulated, or stipulated. Nor can partnerships be purchased, traded or incorporated. Partnerships are voluntarily built between people and organizations that recognize the value in joint collaboration toward a common end. They are fragile entities, which need to be established and maintained by all participants and built upon a foundation of trust.

The Secret Service, by virtue of the protective mission for which we are so well known, has always emphasized discretion and trust in executing our protective duties. Our protective model stresses prevention, and this is achieved through partnerships that we

develop with law enforcement and private industry. We learned long ago that our agency needed the full support and confidence of local law enforcement and certain key elements of the private sector to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we need to maintain a trusted relationship with our protectees so that we can work with them and their staffs to maintain the delicate balance between security and personal privacy.

This long history of discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners. We have successfully investigated many significant cases with the help of our private sector partners, such as network intrusions and compromises of critical information or operating systems. In such cases, even though we have significant technical expertise, we still rely on our private sector counterparts to collaborate with us in identifying and preserving critical evidence to solve the case and bring the perpetrator to justice. Equally important in such cases is conducting the investigation in a manner that avoids unnecessary disruption or adverse consequences to the victim or business. With the variety of operating platforms and proprietary operating systems in the private sector, we could not accomplish these objectives without the direct support of our private sector counterparts. Our ECTFs across the country have been working hard at maintaining and building this trust that has developed between law enforcement, private industry and academia.

Let me share with you some insights regarding an ongoing case that our Omaha Resident Office is investigating in conjunction with our Chicago, New York and San Francisco Electronic Crimes Task Forces. The case, which came to our attention in early February through our contacts in the credit card industry, involves an unlawful intrusion into the computer system of a third-party credit card processor. This company is responsible for processing the credit card transactions of companies such as Visa, MasterCard, American Express and Discover. We believe that multiple machines combined to attack this processor's computer system and unlawfully seize well over 10 million credit card numbers, along with expiration dates, from the company's electronic files.

Our investigation, with the involvement of the Federal Bureau of Investigation, determined that these multiple servers were located both within and outside the United States. The Secret Service is completing electronic forensic examinations and is working with foreign authorities in gathering further evidence concerning this attack.

Mr. Chairman, that concludes my prepared statement, and I would be happy to answer any questions that you or other members of the subcommittees may have.