U.S. DEPARTMENT OF HOMELAND SECURITY

U.S. Secret Service

FOR IMMEDIATE RELEASE **April 3, 2003**
PUB 13-03

U.S. SECRET SERVICE ELECTRONIC CRIMES EXPERTS ADDRESS HOUSE SUBCOMMITTEE ON "FIGHTING FRAUD: IMPROVING INFORMATION SECURITY"

WASHINGTON, D.C. – On Thursday, April 3, 2003, agents from the United States Secret Service testified before a joint U.S. House of Representative subcommittee hearing on the agency's efforts to protect America's financial and critical infrastructure. The House Financial Service Committee's Financial Institutions and Consumer Credit Subcommittee and the Oversight and Investigations Subcommittee hosted the joint hearing titled "Fighting Fraud: Improving Information Security."

Well known for protecting the nation's leaders, the United States Secret Service is also responsible for protecting America's financial infrastructure. The Secret Service has statutory jurisdiction to investigate a wide range of technology-based crimes, including credit and debit card fraud, identity theft, false identification fraud, counterfeit currency and checks, financial institution fraud and telecommunications fraud.

"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," Special Agent in Charge of the Secret Service Financial Crimes Division Tim Caddigan told members of the subcommittees. "There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment."

One successful model, as detailed to the committee, is the Secret Service's Electronic Crimes Task Forces. Based on a model developed in 1995 in New York City, and authorized nationwide with the passage of the USA PATRIOT Act of 2001, the task force approach developed by the Secret Service has generated unprecedented partnerships among federal, state and local law enforcement, the private sector, and academia. These partnerships have experienced remarkable success in detecting and suppressing computer-based crime.

"Our task force model stresses prevention through partnership," Caddigan said. "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 incursion occurs."

The task forces have identified tools and methodologies that can be employed by its partners in the business, academic and law enforcement communities to eliminate potential threats to their information systems. The nine regional task forces – located in New York, Los Angeles, San Francisco, Chicago, Boston, Charlotte, Miami, Las Vegas

-more-

and Washington, D.C. – are 21st century law enforcement models that modernize criminal justice and incorporate partnerships and information sharing within their core competencies.

In addition to the Electronic Crimes Task Forces, members of the subcommittees were briefed on several components of the Secret Service's investigative response to cyber crime, including:

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. 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.

Best Practices Guide to Searching and Seizing Electronic Evidence -- Joining forces with the International Association of Chiefs of Police and the National Institute for Justice, the Secret Service created this guide designed for the first responder, line officer and detective alike. More than 300,000 copies of the guide have been distributed, free-of-charge, to local, state and federal law enforcement.

Forward Edge -- 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. More than 20,000 copies have been distributed.

Critical Systems Protection Initiative (CSPI) -- A collaborative effort between the Secret Service and Carnegie-Mellon University, the CSPI 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.

###

EDITOR'S NOTE: For questions concerning this release, please contact the United States Secret Service Office of Government and Public Affairs at 202-406-5708.