

RESPONSES OF PABLO MARTINEZ

Questions for the Record – Senator Sheldon Whitehouse

To Pablo Martinez, Deputy Special Agent In Charge, Criminal Investigation Division, Cyber Crime Operations, United States Secret Service.

Question:

Per my request at the hearing, please describe the extent to which your organization's cyber security resources are empowered to supplement criminal enforcement efforts with the use of civil injunctive tools to combat cyber security threats.

Response:

In conjunction with our cyber security responsibilities, the Secret Service has no such civil enforcement authority.

Questions for the Record – Senator Dianne Feinstein

Question:

In your testimony, you note that in fiscal year 2010 you opened 957 criminal cases and arrested 1,217 suspects for cyber crime violations.

Can you provide, for each of the last five years:

- The number of arrests for cyber crime offenses of individuals located in Russia?
- The number of individuals located in Russia prosecuted for cyber crime offenses?
- The number of arrests for cyber crime offenses of individuals located in Eastern Europe?
- The number of individuals located in Eastern Europe prosecuted for cyber crime offenses?

Response:

The Secret Service submits the following information in response to the questions listed above:

Fiscal Year	Cases	Arrests	Number of individuals prosecuted in Eastern Europe	Number of individuals prosecuted in Russia
2010	957	1217	44	8
2009	936	1224	45	6
2008	846	1155	11	2
2007	961	789	11	8
2006	934	828	8	9

Questions for the Record – Senator Orrin G. Hatch

Question: (Snow/Martinez) National Cyber Investigative Joint Task Force

Mr. Snow and Mr. Martinez, hackers can simultaneously attack our critical infrastructure.

These hacks impact banking systems, electrical grids, transportation systems and military networks.

However, based on our organizational structure, the responsibility for defending these systems falls to a variety of different agencies. This could give the hacker an advantage unless information is shared.

I am aware that the FBI leads the National Cyber Investigative Joint Task Force. This national center has personnel from a variety of agencies and entities assigned there, including the Secret Service.

What is the dynamic inside the task force? Are agencies cooperating with one another?

Response:

The Secret Service maintains an excellent relationship with the Federal Bureau of Investigation. As one of the four core members, the Secret Service has one full-time agent assigned to the National Cyber Investigative Joint Task Force (NCIJTF). The Secret Service, through this liaison, provides investigative coordination and de-confliction with the NCIJTF partner agencies to improve the Nation's security against the full spectrum of cyber threats. Furthermore, through our participation, the Secret Service is able to share pertinent information related to evolving methodologies and operational strategies to counter criminal and nation-state cyber threats to the national information and financial infrastructure.

For example, during the recent intrusion of the Nasdaq, the Secret Service was able to share information with the FBI and other members of the NCIJTF that benefited the efforts undertaken in the investigation.

Additionally, as a part of the Secret Service's efforts to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following Department of Homeland Security (DHS) and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section

- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

Question: (Martinez) Secret Service National Computer Forensics Institute

Mr. Martinez, your testimony discussed the National Computer Forensics Institute located in Hoover, Alabama. I am aware that this center is utilized to train state and local investigators as well as prosecutors and judges in techniques relating to digital evidence and computer forensics.

1) Currently, how much funding does the Secret Service receive in its annual budget to operate the National Computer Forensics Institute?

Response:

The Secret Service does not receive direct funding in its annual budget to operate the National Computer Forensics Institute (NCFI). Currently, the Department of Homeland Security, via the National Protection and Programs Directorate (NPPD), is providing the Secret Service with \$4 million in annual funding through an interagency agreement.

2) Is the allotted budget amount at a sufficient level to expand and grow the institute at a rate commensurate with growth of cyber crime cases investigated?

Response:

The current funding of \$4 million per year only allows the NCFI to operate at 25% capacity.

3) Would additional funding of the NCFI, and for that matter the ECTFs, enable the Secret Service to maximize outreach to state and local investigators as well as provide more training opportunities for judges, prosecutors and detectives?

Response:

Additional funding would allow for the Secret Service to train additional state and local investigators, judges, and prosecutors through the NCFI. Further, the demand continues to increase due to the lack of accessible training offered to state and local officers, judges, and prosecutors.

For example, in 2010, the Secret Service was only able to accept 23% of all applicants. Operating under the same budget, in 2009, the Secret Service was only able to accept 25% of all applicants. It is important to note that the demand for training continues to increase. Additional funding would also allow for the NCFI to develop curriculum which would meet the demands for training to mitigate against current-day cybercrimes.

ECTFs are the backbone of the Secret Service's ability to fight cyber crime and have been recognized as an established program that is focused on preventing, detecting, mitigating, and investigating cyber attacks against the critical infrastructure of the United States. The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs, which are primarily funded through the Treasury Executive Office for Asset Forfeiture (TEOAF), includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners.

While the ECTF model has demonstrated its value to the Department of Homeland Security's mission of securing this nation's critical infrastructure, the current workload for each is substantial and there is a need for additional ECTFs. The Secret Service is committed to following the direction of Congress, as well as the goals set forth by the Department of Homeland Security, in attempting to enhance and expand programs that are designed to protect and defend America's critical infrastructure.

Question: (Martinez) Secret Service Presence In Future Countries of Cyber Concern

Mr. Martinez, are there countries or regions abroad that the Secret Service has determined to potentially be the future source of cyber crime directed at United States entities or businesses? If so, what countries or regions would the Secret Service like to establish a presence in an effort to train indigenous law enforcement and thwart the development of this nation into a cyber crime haven?

Response:

At no time in history have the challenges been greater for law enforcement. Technological innovations such as e-commerce, on-line banking and trading, the Internet, and electronic payments systems facilitate business but also remain prime targets for organized criminal groups. In recent years, there has been a significant increase in transnational criminal groups that target U.S. banking and other related financial interests.

Joint investigations with our foreign law enforcement partners have resulted in the arrests of hackers who have compromised financial institutions and conducted network intrusions into the Federal Reserve Bank, as well as those who traffic in stolen information. These investigations are made possible by the partnerships our existing offices have forged with their counterparts in law enforcement. Existing partnerships will be strengthened and new partnerships will be forged with an increase in Secret Service presence in offices around the world.

Cyber criminals remain active in Eastern Europe. The Secret Service is in the process of establishing a TDY presence in Ukraine to work with members of the Security Service of Ukraine (SBU) in cybercrime matters. The Service would also like to bolster the number of personnel currently assigned to some of its European offices to combat the threat from cybercrime.

The Secret Service sees a need to enhance and expand our overseas offices by 9 FTEs. This would allow for the Secret Service to permanently staff the Serious Organized Crime Agency (SOCA) Task Force in London, England, and add staff to several foreign offices. SOCA is one of the Secret Service's closest foreign law enforcement partners in the area of electronic crimes. Many of the cases under investigation by the SOCA have targets in common with Secret Service investigations. The Secret Service currently has agents detailed to SOCA and has day-to-day interaction with SOCA officers on cyber investigations in the United Kingdom and the European Union. Permanently staffing SOCA will enhance the ability of the Secret Service to protect U.S. financial interests.

Questions: (Martinez) Authorities and Tools

- 1) Mr. Martinez, are there any additional tools that the Secret Service requires to combat cyber crime both domestically and abroad?**
- 2) Are there any titles or authorities that need to be updated to best meet the investigative demands of the Secret Service both domestically and abroad?**

Response:

The effective relationships we have developed with our international law enforcement partners are attributed to our long-standing commitment to work with the host nation in a cooperative environment. This environment fosters relationships built on trust and mutual respect, and results in the sharing of information and best practices.

The Secret Service has established and supports Vetted Anti-Counterfeiting Forces (VACF) in Colombia. Since 2001, our vetted partners in Colombia have seized over \$262 million in counterfeit U.S. currency, arrested more than 665 suspects, suppressed 113 counterfeit printing plants, and reduced the amount of Colombia-originated counterfeit passed within the United States by more than 70 percent.

Breaking up criminal networks required a highly coordinated law enforcement approach focused on constant innovation in tactics to meet emerging threats. The Secret Service believes that the vetted task force model would lend itself to combat cybercrime, as well. Identifying, training, and equipping cyber criminal investigators from foreign law enforcement agencies would assist the Secret Service in the investigation of cyber criminals located overseas.

The Department of Justice has made several recommendations to the Administration on Cyber Legislation that is being proposed as part of a comprehensive cyber legislative package. The Secret Service supports Department of Justice's proposals for enhancement of 18 USC 1030.

Questions for the Record – Senator Amy Klobuchar

Question: I was interested to read your testimony’s discussion of “carding websites” that serve as forums for bad actors to buy and sell personal financial information among other activities. Are there any additional tools the Secret Service needs to combat these carding sites?

Response:

The Secret Service established the Cyber Investigations Branch, within the Criminal Investigative Division, to combat the rise in cyber crime targeting our nation’s financial payment systems and critical infrastructures. The Cyber Investigations Branch is comprised of several important sections focused on investigating and preventing cyber attacks, including the Cyber Intelligence Section (CIS).

The CIS serves a critical investigative support function; it collects, analyzes, and disseminates data in support of Secret Service investigations nationwide and overseas and generates new investigative leads based upon this criminal information. Furthermore, CIS has developed an investigative unit. It is this unit that actively targets “carding” web sites. They work to identify, locate, and apprehend international cyber criminals involved in cyber intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes, and have directly contributed to the arrests of 41 transnational cyber criminals.

The Secret Service has had tremendous success with its CIS investigative unit, and is hoping to expand its program by hiring, training, and equipping additional analysts with a specific expertise in Eurasian criminal organizations who use the Internet to carry out fraud schemes affecting the critical financial infrastructure of the United States. These analysts would be proficient in Eastern European languages (to include Russian, Polish, and Ukrainian), and Vietnamese.

Furthermore, as cyber criminals continue to explore and employ new technologies, commercial vendors are finding it harder to update their products to address advances among cyber criminals. As a result, law enforcement has turned to custom-built or specialized tools to supplement and complement their investigative approach. The Secret Service is also seeking additional resources to acquire tools to enhance its forensic capability to deal with the growing problem of cryptography, the encryption/decryption of data contained within a computer’s hard drive.