U.S. Immigration
and Customs
Enforcement

STATEMENT

OF

PETER T. EDGE
EXECUTIVE ASSOCIATE DIRECTOR
HOMELAND SECURITY INVESTIGATIONS

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

“Investing in Cyber Security: Understanding Risks and Building Capabilities for the Future”

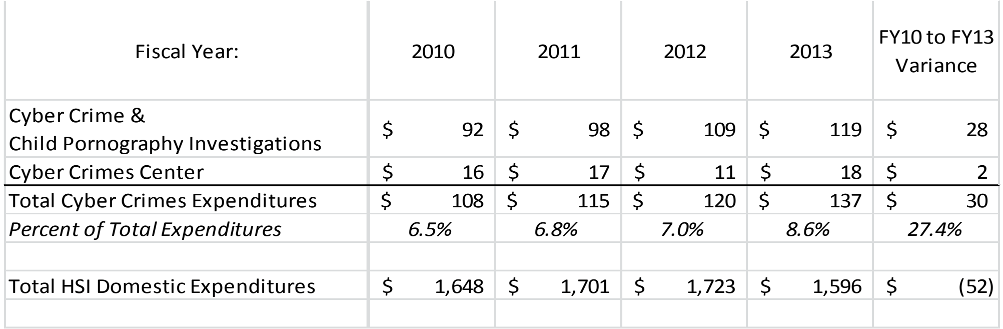
BEFORE THE

U.S. SENATE
APPROPRIATIONS SUBCOMMITTEE ON HOMELAND SECURITY

Wednesday, May 7, 2014
2:00 P.M.
Senate Dirksen Building 192

Introduction

On behalf of the men and women of U.S. Immigration and Customs Enforcement (ICE), thank you for the opportunity to appear before you today to discuss cyber security and the impact ICE’s Cyber Crime Center (C3) makes with respect to protecting our nation's borders and enhancing public safety. C3 has been in existence since 1997 and was created to support the investigative mission of the U.S. Customs Service. Now, 17 years later, C3 is recognized worldwide as a center of excellence in cyber law enforcement. ICE expenditures for Cyber Crime investigations have increased 39 percent since FY 2010. Additionally, Cyber Crimes investigations account for 9 percent of total Domestic Investigations expenditures compared to 6.5 percent in FY 2010.



Fiscal Year:	2010	2011	2012	2013	FY10 to FY13 Variance
Cyber Crime & Child Pornography Investigations	$ 92	$ 98	$ 109	$ 119	$ 28
Cyber Crimes Center	$ 16	$ 17	$ 11	$ 18	$ 2
Total Cyber Crimes Expenditures	$ 108	$ 115	$ 120	$ 137	$ 30
Percent of Total Expenditures	*6.5%*	*6.8%*	*7.0%*	*8.6%*	*27.4%*
Total HSI Domestic Expenditures	$ 1,648	$ 1,701	$ 1,723	$ 1,596	$ (52)

ICE Homeland Security Investigations (HSI) is the principal investigative arm of the U.S. Department of Homeland Security (DHS) and the second-largest federal criminal investigative agency, with broad legal authority to enforce more than 400 federal statutes. HSI has taken a leading role in coordinating domestic and international law enforcement actions among our law enforcement partners through several centers of excellence that we lead – including C3.

The Internet poses a significant challenge to law enforcement. When a criminal never has to meet his victim face to face, but can hide behind what appears to be a legitimate website, consumer fraud runs rampant. When transnational criminal organizations employ technical means to steal intellectual property, American ingenuity is stymied. When money launderers utilize non-traditional, internet-based financial services, circumventing regulatory safeguards, public safety is further threatened. Criminal networks are becoming increasingly sophisticated in taking advantage of the many ways in which the Internet can streamline communications, financing, and logistics – just as it does for legal enterprise. As a consequence, law enforcement agencies must respond by properly preparing investigators for work in cyberspace. As information systems and computer networks become increasingly prolific, the technical challenges facing law enforcement investigations of criminals operating on, or through, the Internet grow daunting, and the considerations in collecting electronic evidence become increasingly complex. A recent HSI enforcement action targeting intellectual property violations saw the deployment of five percent of HSI's Computer Forensics Agents (CFAs) in a single day. These CFAs were tasked with securing the electronic evidence from nine websites, and they will be heavily involved in sorting through the evidence for potential prosecutions

Cyber Crimes Center

C3 brings the full range of ICE cyber investigations and computer forensic assets together in a single location to coordinate global investigations and to provide support to our field offices in their efforts combat cyber-enabled crime. C3 is comprised of three units: the Cyber Crimes Unit, the Computer Forensics Unit, and the Child Exploitation Investigations. The C3 facility houses a cyber investigations training room and a computer forensics laboratory. The Center is staffed by special agents, intelligence research specialists, computer forensics analysts, and mission support personnel. Each of C3's units plays an integral role in supporting investigations of cybercrime and cyber-enabled crime. The scope of these investigations includes any instance where information technology, or computer networks are substantially employed to facilitate international smuggling, money laundering, Internet-based financial frauds or identity theft, proliferation of strategic commodities or the theft of export controlled technical data, and trafficking in child pornography and other child exploitation crimes. The Cyber Crimes Unit and Child Exploitation Investigations Unit provide coordination, de-confliction, resources, training, and subject matter expertise in these investigations. The Computer Forensics Unit oversees the agency's computer forensics program, including the agency's participation in, and contributions to, the Treasury Computer Forensics Training Program.

Cyber Crimes Unit

The Cyber Crimes Unit supports HSI investigations of cyber enabled criminal activities. The Cyber Crimes Unit provides oversight, coordination, de-confliction, resources, and subject matter expertise to HSI offices in the investigation of international smuggling, proliferation, fraud, and money laundering activities where information systems, networks, and the Internet serve as significant facilitating mechanisms for the crime. The Cyber Crimes Unit particularly focuses its efforts towards cyber economic crimes involving financial fraud, the theft of digital intellectual property and technical data controlled under export laws, and the targeting of cross-border illicit internet marketplaces. The Cyber Crimes Unit also works to develop and deliver training to HSI personnel in the investigation of cyber-enabled crimes. The Cyber Crimes Unit further works to support HSI cyber investigations through its Emerging Technology program which focuses on collaborative relationships with other government agencies and academic institutions intended toward development of technical solutions to technical problem sets facing law enforcement.

Emerging Technologies

The Cyber Crimes Unit is also dedicated to the development of tools and capabilities to conduct online cyber investigations. Emerging technology, such as The Onion Router, also known as TOR, or the utilization of virtual currencies, allow the transnational criminal organizations to navigate in cyberspace anonymously. C3 has partnered with DHS Science and Technology to collaborate with academia and other partners to develop tools and best practices, to stay abreast of emerging technologies and continue to lean in to prevent and deter illegal activities.

Virtual Currency

In contrast to traditional currency, monetary instruments, or other methods of transferring value, virtual currencies serve as mediums of exchange, but are not accepted as legal tender in any recognized government jurisdiction. However, virtual currencies can be used to conduct transactions entirely within a virtual economy, transferred between individuals, or used in lieu of a government-issued currency to purchase goods and services.

The appeal of virtual currencies, especially “open” or “convertible” currencies that can be exchanged for traditional currency, and vice versa, is that they may allow value to be transferred much more rapidly and cheaply (especially internationally) than through traditional banking payment systems, and often with greater anonymity and reduced oversight.

ICE has recognized the potential for criminal exploitation and the money laundering threat posed by virtual currency. ICE has, therefore, strategically deployed a multi-prong investigative strategy designed to target illicit virtual currency platforms, currency exchangers, and underground black markets such as "carding," illegal drugs, illegal firearms, and child pornography forums.

ICE recognizes that our approach to combating the illicit use of virtual currency systems must include collaboration and coordination with our domestic and international partners. To that end, ICE works closely with our federal, state, local, and international law enforcement partners, and other members of the interagency.

Recent Investigations

Crack99

Among HSI's broad investigative authority, we are the primary enforcer of the Arms Export Control Act and as such has responsibility to work with industry to safeguard this data from being exploited and smuggled out of the country. This includes the investigation of websites that offer the sale of prohibited items as well as transnational criminal organizations that steal the data without the knowledge of industry.

HSI Philadelphia learned during a private industry outreach meeting, of an online company known as Crack99, believed to be involved in the illegal sale of U.S. manufactured software products. HSI collaborated with Defense Criminal Investigative Services and conducted numerous undercover purchases of stolen software from Crack99. Once payment had been made and accepted in China, the software was posted and received, often compressed into specialty files and then "cracked" to overcome the license restrictions. The software programs were used in multiple design and engineering systems that had a broad range of user applications to include: explosive simulation, aircraft mission simulation, oil field management, antenna design and radio frequency signaling.

Many of the U.S.-manufactured software programs offered by Crack99 were controlled for export and were subject to the Department of Commerce's Export Administration Regulations. The estimated monetary loss of these illegal software sales conducted by Crack99 was valued at approximately $1 million. Crack99 had "cracked" the software of thousands of U.S. businesses.

HSI Special Agents identified the U.S. based servers and seized all accounts, websites and domains associated with Crack99's distribution of stolen software. Two servers and six domain names were seized. The three main suspects were charged, convicted and sentenced for various violations of conspiracy, fraud, smuggling and copyright infringement.

Mt .Gox

In May 2013, through an interagency taskforce led by ICE in Baltimore, Maryland, three U.S. bank accounts associated with what was then the world's largest Bitcoin (a specific virtual currency) exchanger, Japan-based Mt.Gox, were seized for violations of 18 U.S.C. § 1960, operating a money service business in the United States without a license. Some of the funds were linked to the illicit purchase of drugs, firearms, and child pornography. These and many other ongoing criminal investigations have provided ICE with a better understanding of the risks and challenges posed by virtual currencies.

Online Child Exploitation Investigations

ICE has established itself as a world leader in online child exploitation investigations due to the breadth of its authorities and presence throughout the world. Under the auspices Operation Predator, HSI child exploitation investigations focuses on the enforcement, disruption and dismantlement of individuals and groups involved in the possession, receipt, distribution, transportation, and production of child pornography. Since the launch of Operation Predator in 2003, HSI has initiated more than 30,700 criminal investigations; arrested more than 10,900 child predators; and contributed to more than 8,000 indictments and criminal convictions for child exploitation violations. In FY 2013 alone, our agency was responsible for over 2,000 criminal arrests relating to child exploitation, while launching in excess of 4,000 child exploitation investigations worldwide, both new records for HSI. In FY 2013, there were 927 children identified as victims during the course of ICE HSI-led or joint child exploitation and/or child sex tourism investigations. Key to HSI's fight against child exploitation is HSI's C3. C3 directs HSI in its mission to investigate large-scale producers and distributors of child pornography, as well as individuals who travel abroad for the purpose of engaging in sex with minors, also known as Child Sex Tourism (CST). C3 employs the latest technology to collect evidence of persons and organized groups who sexually exploit children through the use of websites, chat rooms, newsgroups and peer-to-peer trading. C3 also provides assistance to HSI field offices, coordinates major investigations, and conducts undercover operations throughout the world to identify and apprehend violators.

Operation Round Table

In March 2014, HSI completed the largest online child exploitation investigations in ICE's history, involving victims in 39 states and five countries. Fourteen men operating a child pornography website on the Darknet's Onion Router (TOR) were arrested and charged as part of a conspiracy to operate a child exploitation enterprise, following an extensive international investigation by HSI and the U.S. Postal Inspection Service (USPIS).

To date, investigators have identified 251 minor victims in 39 states and five foreign countries: 228 in the United States and 23 in the United Kingdom, Canada, New Zealand, Australia and Belgium. Eight of the victims were female and 243 were male. The majority of victims, 159, were 13 to 15 years old; 59 victims were 16 and 17; 26 victims were 10 to 12; four victims were 7 to 9; one victim was 4 to 6; and two victims were 3 years old or younger. All victims have been contacted by law enforcement and U.S. victims have been offered support services from HSI victim assistance specialists.

Victim Identification Program

Although the traditional law enforcement goal in combating child exploitation is normally viewed to be "arresting and prosecuting predators," the true goal is to protect children. In furtherance of this goal, HSI launched the Victim Identification Program (VIP) in December 2011. Its mission is to combine technological and investigative capabilities and resources to rescue child victims of sexual exploitation. The VIP is a simple idea that combines traditional investigative techniques with cutting edge technology for the purposes of rescuing child victims of sexual exploitation. The victim identification process starts with the discovery of new child abuse material (images, video, and/or audio) that depicts an unidentified minor or minors being sexually abused. HSI analyzes and enhances the material in order to identify clues that may lead to the identity of the victim, suspect or geographic location. When enough clues come together to form a viable lead, the lead is sent out to the appropriate HSI field office for follow-up investigation. During its first two years of operation, the VIP has been responsible for more than 180 victims identified and/or rescued from around the country. HSI is increasingly shifting its focus and dedicating more of its time and resources towards identifying and rescuing the victims of child sexual exploitation and the prevention of these crimes. This focus on victims is not in conflict with ongoing efforts to arrest and prosecute the perpetrators of these horrendous crimes as the identification of victims often leads to the arrest of their abusers.

Project iGuardian

In April 2014, ICE launched an educational outreach program called Project iGuardian, in conjunction with the National Center for Missing & Exploited Children's NetSmartz and the Internet Crimes Against Children (ICAC) Task Forces. Project iGuardian is an outreach awareness program that aims to educate kids, teens, and parents about online safety and how to stay safe from online sexual predators. HSI recognizes the importance of education and community awareness regarding the dangers of online activity. Project iGuardian aims to counter a disturbing fact: many online child predators are able to find victims online because children are not aware of how dangerous online environments can be.

Virtual Global Taskforce

ICE is a founding member and the U.S. representative of the Virtual Global Taskforce (VGT), an international alliance of law enforcement agencies and private industry sector partners working together to prevent and deter online child sexual abuse. In December 2012, HSI was appointed chair and secretariat of the VGT. The Deputy Assistant Director of C3 assumed the duties of chair for a three (3) year tenure. At the same time HSI was appointed the chair, the VGT also agreed to include investigations of CST into its portfolio.

Operation Predator - Smartphone App

In September of 2013, HSI launched a new smartphone app, the first of its kind in U.S. federal law enforcement, designed to seek the public's help with fugitive and unknown suspect child predators. All tips can be reported anonymously through the app, by phone or online, 24 hours a day, seven days a week. In many cases, HSI has been able to make an arrest just hours after issuing a nationwide plea for public assistance. These cases demonstrate the power of the press, social media and the general public in helping solve cases.

Computer Forensics Program

C3 operates and maintains a robust computer forensics program. HSI computer forensic agents/analysts (CFAs) support all HSI investigations involving the use of digital media, as well as provide support to federal, state and local law enforcement upon request.   The computer forensic program is currently comprised of approximately 250 CFAs located in over 110 domestic and foreign HSI offices. The CFAs operate in various environments, supporting investigations to include advanced mobile device data extraction, hard drive repair, data mining of large multi-terabyte data sets, password decryption, border search of electronic devices and on-scene computer forensic assistance. For example, HSI CFAs were instrumental in the seizure of closed circuit video systems that were used in the identification of the Boston Marathon bombing suspects and provided key support for the analysis of suspect media related to Operation Round Table detailed above.

In fiscal year 2013, HSI CFAs encountered approximately 3.9 Petabytes of data (equal to approximately 62 billion pages of image files or 71 billion pages of power point files) and analyzed over 4,400 mobile devices; this is a 45% increase in the volume of data encountered and a 35% increase in the number of mobile devices analyzed from the previous fiscal year.

HSI is a founding member of the Treasury Computer Forensic Training Program (TCFTP), which is a joint computer forensic training initiative between HSI, the U.S. Secret Service and the Internal Revenue Service-Criminal Investigations. Management of the training program rotates every two years, with HSI responsible for administering the program for 2014 and 2015. For 2014, it is anticipated that approximately 200 individuals will receive basic or advanced computer forensic training through the joint training program. This program was designed to provide CFAs operating in the field with the skills necessary to support the ever changing environment of the computer forensic requirements for HSI's investigative mission. In addition to providing training through the TCFTP, the computer forensic program regularly provides computer forensic training for capacity building efforts to foreign law enforcement.

Human Exploitation Rescue Operative Chile Resuce Corps

In April 2013, ICE, entered into a partnership with U.S. Special Operations Command and the National Association to Protect Children (PROTECT) to launch the "Human Exploitation Rescue Operative (HERO) Child Rescue Corps" program. The 12-month internship program is a highly competitive, highly selective non-paid internship, designed for wounded, injured and ill Special Operations Forces to receive training in high-tech computer forensics and law enforcement skills to assist HSI and law enforcement in their efforts to combat child sexual exploitation. Upon successful completion of the training, HERO participants are embedded into computer forensic analyst positions within HSI offices to receive on-the-job training experience. Fifteen HERO participants of the inaugural class have successfully completed all aspects of the program thus far and HSI in in the process of extending offers of employment to all 15 individuals under the Veterans' Recruitment Appointment authority. The HERO program is in the process of recruiting, interviewing and selecting candidates for the 2nd HERO class, which is scheduled to begin in August 2014.

DHS Secretary's Honors Program-Cyber Student Initiative

The DHS Cyber Student Volunteer Initiative, introduced in 2013 by DHS and HSI, offered college students majoring in a cyber-security-related field an unpaid volunteer position to gain invaluable hands-on experience at a DHS component agency. HSI was the sole DHS component to participate in the inaugural program, which was designed to provide high-performing students with challenging work projects, real-life learning scenarios, and mentoring from cyber-security professionals at various HSI field offices. Based on the success of the program, DHS and HSI offered the Student Volunteer Initiative program again in 2014, which was expanded to include new volunteer opportunities at the U. S. Secret Service, the U.S. Coast Guard, the Transportation Security Administration, the Office of Intelligence and Analysis, the DHS Office of the Chief Information Officer, and state and major urban area fusion centers.

Conclusion

Thank you again for the opportunity to appear before you to highlight ICE's Cyber Crime Center and the significant role we contribute in combatting transnational criminal organizations operating in cyberspace and in an increasingly more complex and sophisticated virtual reality. As the cyber world and other new virtual technologies continue to evolve, ICE will remain vigilant and adapt its investigative tools and techniques to dismantle those criminal organizations that use this platform to hide illicit activity.