Testimony of

Lt. Robert Moses

April 16, 2008

Testimony of Lt. Robert Moses
Delaware State Police
Senate Judiciary Subcommittee on Crime and Drugs
"Challenges and Solutions for Protecting our Children from Violence and Exploitation in the 21st Century"
Wednesday, April 16, 2008, 2:00 PM
226 Dirksen Senate Office Building

Good afternoon Chairman Biden and Raking Member Sessions. My name is Lt. Robert Moses. I am the officer-in-charge of the Delaware State Police High Technology Crime Unit and the commanding officer of the Delaware Child Predator Task Force. Thank you for the opportunity to discuss a most successful law enforcement program; the Internet Crimes Against Children Task Force.

I am particularly honored to be here with you and some of my peers in law enforcement. The dedication, knowledge and skills of agents around the nation -- along with federal funding assistance -- have helped to make the ICAC program a success in Delaware and across the country. In particular, Flint Waters of the Wyoming ICAC has led the charge in the efforts against Child Sexual Exploitation. His vision and technical skills have provided law enforcement agencies world-wide with Operation Fairplay. Operation Fairplay software allows law enforcement to proactively identify criminals who possess and distribute child pornography. This software tool enhances our ability to quickly arrest and prosecute sexual predators.

In the past, proactive undercover cases were only developed by officers communicating with predators in chat rooms and other Internet forums. These cases required hundreds of hours of investigative effort and caused unique legal and investigative challenges. In reality, only a small fraction of the predators were actually identified through that investigative method because law enforcement simply did not have enough time or the right resources to reach them. Thanks to Flint, and the dedicated men and women of the Wyoming ICAC, we now have an additional weapon in our fight against child sexual offenders that allows us to more efficiently and effectively identify more predators and take them off the streets.

By using the Wyoming ICAC software to target individuals who possess and distribute child pornography, we will have a profound effect on the safety of our children by saving them from the physical and psychological trauma of sexual abuse. To be clear - possessors of child pornography are predators. But moreover, research has shown that that at least 30% of all individuals who possess child pornography have had sexual contact with a child, as well.

We see these cases in Delaware all the time. One instance involved a father of an 18 month old male who videotaped himself sodomizing his baby. We have encountered a child therapist who counsels children with sexual disorders abusing his clients and downloading child pornography. We have investigated and prosecuted police officers who possessed child pornography.

You have just seen a sampling, but even that could not prepare you for the shocking nature of the violent, degrading pornography we see every day in our investigations. Pedophiles often use these materials for their own sexual arousal and gratification. In a process known as "grooming," predators use graphic materials to lower the inhibitions of children they are attempting to seduce. The predators use the same materials in an effort to arouse children or to demonstrate the desired sexual acts. It cannot be forgotten that each time a graphic image moves on the Internet, the child in the photograph is being re-victimized.

Today, electronic crime investigations of child sexual exploitation can pose unique and difficult challenges to law enforcement. The technical nature of computer hardware and software, as well as the Internet and other forms of electronic communication are very complex. Sex offenders today communicate with children and transmit child pornography images using various techniques to conceal their electronic footprints. Investigators must deal with not only the complicated technical, legal and jurisdictional issues when the Internet and computers are involved, but also need highly trained and equipped individuals to conduct the forensic examination of the electronic media seized. The forensic examiner provides the evidence necessary for the prosecution of online sexual exploitation investigations, and also develops other investigative leads pointing to the identity of other victims or other suspects.

To illustrate this point, the Delaware ICAC received three "Cybertips" from the National Center for Missing and Exploited Children regarding an individual who sent child pornography images via email. Investigation revealed the sender of the email was Paul Thielemann, of Georgetown, Delaware. A search warrant was executed at Thielmann's residence and two computers and other electronic media were seized. A forensic examination revealed images and videos of sexually abusive images of children, as well as nearly 3,000 online chats between Thielemann and several other individuals. These chats were discussions of their desire to have sex with children as young as 18 months old. As a result of our investigation, nine suspects were ultimately turned over to the United States Attorney's Office to be prosecuted under federal laws that call for harsher penalties than current Delaware statute. Five children were rescued.

There are many success stories, but the lack of skilled computer forensic examiners, equipment, and lab facilities create a burden on law enforcement because it prevents the timely investigation and prosecution of electronic crimes. In response to these factors and the increased sophistication of technology challenging Delaware law enforcement in their investigation of electronic and computer crimes, in June of 2001 the Delaware State Police established the High Technology Crimes Unit (HTCU). Since its creation, the HTCU has seen a significant increase in requests from state and local law enforcement agencies for the forensic analysis of electronic media that contains evidence of online child sexual exploitation. Furthermore, due to the increased size of hard drives, the different types and the increased numbers of electronic media being seized, these examinations require much more time. Computer hard drives can now be inexpensively purchased in sizes up to 1000 GB. To put a Gigabyte (GB) into perspective, a 12 GB hard drive

can contain approximately 4,300,000 pages. If stacked, those pages be would equal to 1,431 feet. In comparison, the Sears Tower in Chicago stands 1,450 feet tall. And these predators are filling their hard drives with evidence of child sexual abuse.

Advances in technology present the computer forensic specialist with continually evolving challenges. It is essential that forensic computer examinations be conducted by properly skilled and qualified staff who have the appropriate equipment and training. On average it takes 12 to 18 months and costs approximately $40,000 to fully equip and train a new forensic examiner. Additionally, given that technology is continually advancing, it is important that the examiner receive ongoing training and equipment upgrades.

In Delaware we now have a statewide Child Predator Task Force that streamlines the efforts of federal, state, and local law enforcement to proactively go after child predators and possessors of pornography. The Task Force was initially formed as the Delaware Internet Crimes Against Children Task Force in June 2007 as a partnership between the Delaware State Police, the Delaware Department of Justice, and the U.S. Attorney's Office. After receiving at $250,000 federal ICAC grant last October, the Task Force secured additional training and equipment that is used by prosecutors and investigators who now work side by side in the Task Force headquarters. The Delaware Child Predator Task force is the central hub for coordinating online child sexual exploitation cases across the entire state.

Additionally, the federal funding provided to Delaware law enforcement has enabled us to develop a coordinated approach to reducing the incidences of online sexual exploitation. Along with the previously mentioned agencies and with the help of the FBI, U.S. Immigration and Customs Enforcement, the National Center for Missing Exploited Children, and the 59 ICAC Regional Task Forces, we now have the resources and coordination necessary to develop an effective strategy to prevent, indentify, investigate and prosecute online sexual predators.

The demands for fighting back against online sexual exploitation are extensive and will continue to increase dramatically as technology evolves. With continued federal funding and support, the Internet Crimes Against Children Program will continue to navigate this fast-changing terrain in an effort to outpace those who use computers and the Internet to victimize our children.