Global Alliance Against Child Sexual Abuse Online - 2014 Reporting Form

UNITED STATES

Policy Target No. 1

Enhancing efforts to identify victims and ensuring that they receive the necessary assistance, support and protection.

Operational Goal: Increase the number of identified victims in the International Child Sexual Exploitation images database (ICSE database) managed by INTERPOL by at least 10% yearly.

A) Please report on implementation of any measures announced in your country's 2013 report

See below

B) Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance

The Child Exploitation Investigations Unit of the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Cyber Crimes Center (C3), operates the Victim Identification Program (VIP), which was launched in December 2011. 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. In 2014, DHS-ICE-HSI trained and equipped twelve of its regional offices to participate in the VIP. The VIP combines old-fashioned 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 that depicts the sexual abuse of an unidentified minor or minors. 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, a lead is sent out to the appropriate HSI field office for follow-up investigation.

The National Child Victim Identification System (NCVIS), version 2, which is owned by DHS-ICE-HSI, is an application that assists federal, state, local, and international law enforcement agencies in the investigation and prosecution of child exploitation crimes, specifically those involving images of child sexual exploitation. NCVIS 2 maintains a repository of digital images of child exploitation seized and/or submitted for comparison by law enforcement agencies. HSI has expanded the scope of system information that is shared with external law enforcement agencies that maintain their own databases of child exploitation crimes for the purposes of identifying the child victims and supporting law enforcement investigations and prosecutions into these crimes.

In Fiscal Years 2013 and 2014 (to date), DHS-ICE-HSI's investigations of child exploitation

offenses resulted in the identification of, respectively, 927 and 1,035 victims.

"Project Vic" is intended to promote the investigation of child pornography images that depict unidentified victims, improve the quality of law enforcement-exchanged data, standardize law enforcement data formats, and promote data exchange efforts in child pornography investigations. The project's participants consist of U.S. federal and state law enforcement agencies, the International Centre for Missing & Exploited Children (ICMEC), NetClean, Microsoft, Hubstream, Thorn, and the University of Illinois at Chicago. The project relies on the use of robust, updated forensic and image categorization tools and new technologies in order to allow computer forensic analysts to review and analyze computer media containing large collections of child pornography in a more automated and efficient manner. As a result, child pornography images that depict victims who have not been identified can be more easily isolated for further investigation. In 2014, Project Vic trained over 300 students through in-person, hands-on training courses, and it has reached hundreds of law enforcement personnel through webinars available in the U.S. and throughout the world. Several international partners have been trained in the use of Project Vic tools and data. In September 2014, the first Project Vic International Tech Summit was held with participants from several U.S. agencies (HSI, Federal Bureau of Investigation, U.S. Postal Inspection Service, Internet Crimes Against Children (ICAC) Taskforces), international partners (UK, Australia, New Zealand, Canada), industry partners (NetClean, BlueBear, Ziuz, Magnet Forensics, Hubstream), and non-governmental organizations (ICMEC, NCMEC, Thorn). In 2014, Project Vic initiatives resulted in the adoption of Open Data ("OData") protocols and Project Vic compliance in numerous law enforcement and forensic tools including: Magnet Forensics Internet Evidence Finder, Autopsy Forensic, Xways Forensics, NetClean Analyze DI, Blue Bear LACE, Ziuz Vizx, Nuix Forensics, and PenLink; and has made great progress with Access Data for use in FTK. Project Vic via Hubstream currently manages and maintains a hash cloud for Project Vic hashes. Through an established partnership with ICAC Child Online Protective Services (ICACCOPS) and DOJ, all credentialing and access to the hashes is facilitated via the ICACCOPS website.

In 2008, the Federal Bureau of Investigation (FBI) launched "Operation Rescue Me," a program which remains focused on utilizing image analysis to determine the identity of child victims depicted in child sexual exploitation material. While most FBI investigations generally focus on obtaining leads and other information necessary to identify/prosecute subjects and offenders, the image analysis methods employed through Operation Rescue Me involve a concentrated effort to identify and subsequently rescue abused children. Since the program's inception, Operation Rescue Me has been responsible for the identification of 73 child victims depicted in numerous child pornography series being traded on the Internet. Candidate images for Operation Rescue Me arise from new child pornography series discovered by FBI field investigations, from forensic exams, or from nominations by NCMEC.

In 2004, the FBI began its Endangered Child Alert Program (ECAP), a new proactive approach to identifying unknown individuals involved in the sexual abuse of children and the production of child pornography. A collaborative effort between the FBI and NCMEC, ECAP seeks national and international exposure of unknown adults (referred to as John/Jane Does) whose faces and/or distinguishing characteristics are visible in child pornography images. These faces and/or distinguishing marks *(i.e.,* scars, moles, tattoos, etc.) are displayed on the "Seeking Information" section of the FBI website as well as various other media outlets in the hope that someone from the public can identify them. As a result of ECAP, the faces of many Jane/John Does have been broadcast on U.S. television shows such as America's Most Wanted, America Fights Back, The

Oprah Winfrey Show, and the O'Reilly Factor. Since the inception of ECAP, 28 John/Jane Does have been investigated, 22 of which have been successfully identified and subsequently prosecuted.

In 2013, the U.S. Department of Justice (DOJ) committed to co-chairing a one-year joint government taskforce with the UK Home Office to find new technological solutions to reduce child pornography and other online child exploitation crimes. The UK/US Taskforce to Counter Online Child Exploitation was co-chaired by the Assistant Attorney General for DOJ's Criminal Division and the UK Minister for Policing, Criminal Justice, and Victims. The Taskforce called for the creation of a separate Industry Solutions Group, comprised of industry experts, to identify, design and, where possible, build new technical solutions to address these crimes. The Industry Solutions Group was chaired by the UK Business Ambassador for Digital Industries, Joanna Shields, who previously worked for Google and Facebook, and is currently the chairperson of Tech City UK. The Industry Solutions Group currently operates under the brand "WePROTECT." On May 20-21, 2014, the WePROTECT Technology Solutions Event, which was organized as part of the Taskforce's work, occurred in London and was attended by 67 technical engineers/staff from 48 companies from the internet and digital industry. The purpose of the event was to create an opportunity for industry members to learn about and discuss the problem of online child exploitation; specifically, the sharing of child pornography online, and adults interacting with children online for sexual purposes. The attendees then brainstormed and worked on developing potential technical solutions that could address these problems. As a result of this event, eight "concepts" were identified as potential solutions. The UK Home Office took the lead in building industry support and establishing working groups to further develop and test these ideas from the WePROTECT event in order to determine if they were viable.
Currently, seven of the concepts are divided between five active working groups. One working group is working on two concepts that are specifically directed at helping to identify victims: (1) Harnessing Swarm Intelligence to Identify Victims. Volunteers download an industry-developed application that would use the processing power and bandwidth of volunteers' devices to scan public internet content and calculate facial templates for all images found. Through a secure and central server, using image filtering and facial recognition technology, child pornography would be compared to legal images of children found on the internet in an effort to identify victims; and (2) Audio-visual Analytical Tool to Assist in Victim Identification. Details contained in child pornography *(e.g.*, wallpaper in background) are compared with publically available data to help identify the location depicted in the image, the time the image was taken, or to whom the photographic equipment belonged. This would exploit web-crawlers and processes that continuously populate a database with information from submitted intelligence, freely available images, and metadata from internet sources.

Supported by DOJ grant funding, the National Center for Missing and Exploited Children (NCMEC) works closely with law enforcement officers in combating child exploitation. Law enforcement officers submit images and movies of children seized in child pornography cases to NCMEC's Child Victim Identification Program (CVIP) for review. This program has a dual mission: (1) help prosecutors get convictions by proving that a real child is depicted in child pornography images; and (2) assist law enforcement in locating unidentified child victims. The materials submitted are then screened through the Child Recognition and Identification System

(CRIS), a specialized computer software program designed to efficiently determine which seized content appears to contain identified children. While reviewing contraband, CVIP analysts closely examine the images and videos submitted by law enforcement and document any clues that may lead to the location of an unidentified child victim. Once a location has been determined, the appropriate law enforcement agency may begin an investigation to rescue the child. Many children have been rescued from ongoing exploitation as a result of the cooperative efforts between CVIP and law enforcement.

With approval of law enforcement, NCMEC provides images/videos of identified victims to INTERPOL for inclusion in the ICSE images database. As of the end of year 2014, CVIP documented more than 7,800 identified child victims and NCMEC analysts have analyzed more than 130 million child sexual abuse images/videos.
NCMEC operates a Child Victim Identification Lab where eligible law enforcement users are able to view background identifiers and audio clues from ongoing child pornography cases in the hope that these items may be recognizable or familiar to participants. The system allows users to post comments and suggestions. More than 7,000 authorized users have participated in the Victim Identification Lab and more than 5,600 comments have been collected.

Supported by DOJ grant funding, the National Children's Alliance is the membership and accrediting organization for more than 800 children's advocacy centers (CACs) in the U.S. that provide services to more than 290,000 child abuse victims each year. CACs were originally developed to assist child sexual abuse victims, but that work has now grown to encompass many forms of maltreatment, including commercial sexual exploitation and child pornography trafficking. CACs work closely and collaboratively with law enforcement, child protective services, medical providers, mental health providers, and victims' advocates to ensure offenders are held accountable and children receive the services needed to heal from the trauma of abuse. National Children's Alliance provides consultation for international CAC development efforts, and has been instrumental in the growth and development of CACs around the globe.

Supported by DOJ grant funding, the National Children's Advocacy Center (NCAC) is one of the leading organizations in the world providing training and technical assistance to child abuse response professionals. More than 70,000 child abuse professionals from all 50 states in the U.S. and 33 countries have been trained by the NCAC, with training and technical assistance focusing on development of national policies providing for the protection of children, implementation of the multidisciplinary response model for child abuse, and development of national training programs.

C) Please indicate specific actions that your country will undertake as a_ follow-up

Through the UK/US Taskforce to Counter Online Child Exploitation, DOJ will continue to support the WePROTECT working groups in their efforts to implement the developed concepts. DOJ will continue to fund programs and initiatives that help identify child pornography victims and provide assistance, support and protection to child victims. In order to increase victim identification and protection efforts, DHS-ICE-HSI plans to expand VIP to its remaining fourteen regional offices over the next two years. Twelve Project Vic trainings are scheduled to occur in the U.S. in 2015.

Policy Target No. 2

Enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders.

Operational Goal: Establish the necessary framework for the criminalization of child sexual abuse online and the effective prosecution of offenders, with the objective of enhancing efforts to investigate and prosecute offenders.

A) Please report on implementation of any measures announced in your country's 2013 report

See below.

B) Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance

The FBI is investigating child pornography websites on the "Darknet," which are networks of Internet technologies and platforms that provide anonymity for users (e.g., TOR). On one such website, members advised others on best practices to prevent detection by law enforcement, including advice about the proper use of encryption software, techniques to hide or password-protect child pornography collections, and programs to remove data from a user's computer. To address this threat, the FBI developed innovative strategies, and is leading a global effort through its international task force and partnerships, to identify offenders using anonymity platforms to engage in the sexual abuse of children. To date, the FBI investigation and takedown of the website resulted in the conviction and sentencing of the website's administrator and five co-conspirators for child pornography offenses, with the average sentence being over 20 years. In fiscal years 2013 and 2014, FBI investigations of child exploitation offenses resulted in 2,538 domestic arrests and 1,906 convictions.

Beginning in November 2011 and continuing through May of 2012, the U.S. Postal Inspection Service successfully dismantled an online child exploitation enterprise that began in 2000. Their investigation revealed that dozens of individuals, located throughout the United States and abroad, were members of online, password-protected chat rooms that were dedicated to the distribution, receipt and possession of child pornography. Members used these chat rooms to discuss and promote the sexual exploitation of children and to expand their child pornography collections. Furthermore, the members of the enterprise used a variety of file-sharing servers, as well as high-level data encryption strategies, in an effort to evade law enforcement. Dozens of children around the world were identified as victims of abuse during this investigation. Throughout 2013 - 2014, eleven members of the enterprise were convicted of various child pornography offenses, including child exploitation enterprise.

DOJ funds and provides training to Internet Crimes Against Children (ICAC) Task Forces located in every state of the United States. The ICAC program is a national network of 61 coordinated task forces representing over 3,000 federal, state, and local law enforcement and

prosecutorial agencies, who are responsible for developing an effective response to cyber-enticement and child pornography cases. These agencies are engaged in proactive investigations, forensic investigations, and criminal prosecutions. Since 2009, ICAC Task Forces have provided training to over 226,000 people, including law enforcement officers, forensic interviewers, computer forensic examiners, prosecutors, and others. The Task Forces have conducted well over 200,000 investigations into over a quarter million complaints of child exploitation. These efforts have resulted in the arrests of over 33,000 people.

Key to DHS-ICE-HSI's fight against child exploitation is its Cyber Crimes Center (C3), Child Exploitation Investigations Unit (CEIU). The CEIU leads HSI's mission to investigate 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). The CEIU employs the latest technology to collect evidence and track the activities of individuals and organized groups who sexually exploit children through the use of websites, chat rooms, newsgroups and peer-to-peer trading. The CEIU provides assistance to ICE field offices, coordinates major investigations, and conducts undercover operations throughout the world to identify and apprehend violators. In Fiscal Years 2013 and 2014 (to date), DHS-HSI's investigations of child exploitation offenses resulted in, respectively, 1,241 and 1,410 convictions.

In September 2013, DHS-ICE-HSI launched a new smart phone application - the first of its kind for U.S. federal law enforcement - designed to seek the public's help in apprehending fugitive and unknown suspected child predators. All tips can be reported anonymously through the application, 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 law enforcement to attack crime.

NCMEC's Law Enforcement Services Portal (LESP) allows law-enforcement officers and prosecutors to perform an initial hash value comparison of files seized during child pornography investigations. There are more than 2,600 active users of the LESP and more than 36 million hashes have been compared via the tool.

C) Please indicate specific actions that your country will undertake as a follow-up

U.S. law enforcement will continue to aggressively target national and international online child exploitation offenders for investigation and prosecution, including online groups and offenders who use TOR and other sophisticated, online technology to commit and conceal their crimes. DOJ will continue to fund the ICAC task forces.

Operational Goal: Improve the joint efforts of law enforcement authorities across Global Alliance countries to investigate and prosecute child sexual abuse online.

A) ***Please report on implementation of any measures announced in your country's 2013 report***

See below.

B) ***Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance***

The FBI's Violent Crimes Against Children International Task Force (VCACITF) became operational in 2004 and serves as the largest task force of its kind in the world. The VCACITF consists of a select cadre of child sexual exploitation investigators from around the world and includes more than 60 active task force officers from 38 different countries, including the United Kingdom, Brazil, France, Finland, Australia, Thailand, the Philippines, China, Latvia, Germany, the Netherlands, New Zealand, Canada, Sweden, Russia, Cyprus, Taiwan, Denmark, Belgium, Mexico, Panama, South Africa and Italy. Each year the task force hosts a session that brings newly invited task force officers to the United States to attend a five-week training session where they work side-by-side with FBI special agents in the Major Case Coordination Unit.
International task force officers remain an integral part of the task force once they return to their home countries. The VCACITF has furthered strategic global partnerships through the real-time sharing of intelligence and lead information between task force participants. The VCACITF also conducts an annual case coordination meeting where task force members come together in a central location to share best practices and coordinate transnational investigations between its member countries.

Operation Kilo Hunter, a coordinated effort initiated in 2012 between the FBI and Australian representatives from the FBI's VCACITF, targeted an electronic communications-based international child sexual abuse network with over 100 U.S.-based subjects and over 600 additional subjects around the world. To date, 27 child victims have been rescued. The average age of the rescued children was 6 years old. The majority of the victims were sexually assaulted by family members, to include parents, step-parents and grandparents.
The U.S. continues to participate in the Virtual Global Taskforce (VGT), which is comprised of international law enforcement agencies and private sector partners from around the world working together to fight child abuse online. The VGT strives to make the Internet a safer place; identify, locate and help children at risk; and hold perpetrators accountable. The VGT was established in 2003 and includes the U.S. (DHS-ICE-HSI), United Kingdom (National Crime Agency), Canada (Royal Canadian Mounted Police), Australia (Australian Federal Police), Italy (Postal and Communication Police Service), the United Arab Emirates (Ministry of Interior), Colombia (National Police of Colombia), the Netherlands (Dutch National Police), New Zealand (New Zealand Police), Republic of Korea (Korean National Police Agency), Switzerland (Cybercrime Coordination Unit), EUROPOL, and INTERPOL as its current members. The VGT is intended to augment, not supplant, existing law enforcement initiatives and international relationships related to child exploitation issues. DHS-ICE-HSI is the exclusive U.S. representative to the VGT, and serves as the VGT's current chair.

NCMEC's CyberTipline receives leads and tips from the public and electronic service providers (ESPs) regarding suspected crimes of child sexual exploitation. The CyberTipline is authorized by Congress and operated in partnership with the FBI, DHS-ICE-HSI, the U.S. Postal Inspection Service, ICAC task forces, U.S. Secret Service, DOJ's Child Exploitation Obscenity Section (CEOS), as well as other state and local law enforcement entities. More than 3 million reports of suspected child sexual exploitation have been made to the CyberTipline since its inception in

1998. Reports are continuously triaged to help ensure children in imminent danger get first priority. In coordination with NCMEC, HSI established Virtual Private Network (VPN) connections in several ICE Attaché offices as well as numerous national police forces to facilitate the distribution of CyberTipline reports to law enforcement agencies in more than 95 countries. Several VGT member law enforcement agencies (including Australia, Canada, Italy, Netherlands, New Zealand and the United Kingdom) have established their own VPN connection with NCMEC's CyberTipline to allow direct referrals of CyberTipline reports with an apparent nexus to that country. Hundreds of thousands of referrals are made to international law enforcement agencies each year.

In 2012, NCMEC provided Interpol-NCB Washington with direct access to the entire CyberTipline. Interpol-NCB Washington has the ability to isolate reports by country and make direct CyberTipline referrals to NCB offices around the world. In March 2014, Interpol-NCB Washington began retrieving a daily automated stream of all CyberTipline reports that NCMEC has been unable to refer to a foreign law enforcement entity (e.g., a country without existing VPN coverage). In 2014, several hundred thousand referrals were provided by NCMEC to Interpol-NCB Washington.

Through the U.S.'s participation in the G8 Roma-Lyon Group Law Enforcement Projects Sub-Group, the U.K. and the U.S. organized the Global Symposium on Preventing the International Sexual Exploitation of Children, which the U.K. hosted in London on October 7-9, 2013. The symposium, which was attended by law enforcement officers and representatives of the G8 countries, focused on transnational sex offenders victimizing children, including offenders who utilize the internet to live-stream the sexual abuse of children in other countries. Presentations were linked to workshops and plenary sessions that enabled delegates to discuss offense conduct in their countries and how such conduct is investigated and prosecuted.

C) Please indicate specific actions that your country will undertake as a follow-up

The U.S. will continue to work closely with its international law enforcement partners through the VCACITF, VGT, and other initiatives to investigate and prosecute online child sexual abuse offenders. The U.S. will continue to advocate, during its term as leader of the Global Alliance, for the adoption of policy measures by all Global Alliance members that will enable more timely, comprehensive, and effective information-sharing among international law enforcement partners.

Policy Target No. 3

Enhancing efforts to increase public awareness of the risks posed by children's activities online, including grooming and self-production of images that results in the production of new child pornography that may be distributed online.

Operational Goal: Develop, improve, or support appropriate public awareness campaigns or other measures which educate parents, children, and others responsible for children regarding the risks that children's online conduct poses and the steps they can take to minimize those risks.

A) Please report on implementation of any measures announced in your country's 2013 report

See below.

B) Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance

The FBI's Safe Online Surfing (S.O.S.) Program is a national Internet safety program designed to help students recognize potential dangers associated with the Internet, email, chat rooms and social networking sites. The website for the program was launched in October 2012. The program addresses and defines topics serious in nature, such as seduction, child pornography, solicitation, exploitation, obscenity and online predators. Students take web-based quizzes and review specific web sites aimed at promoting online safety. Since October 2012, more than 176,000 students from around the country have completed the program. More information regarding S.O.S. can be found at: https://sos.fbi.gov/.

In 2014, DHS-ICE-HSI launched an educational outreach program called Project iGuardian, in conjunction with NCMEC's NetSmartz and the ICAC Task Forces. Project iGuardian aims to educate kids, teens, and parents about staying safe from online sexual predators, who exploit juveniles' naivety regarding the danger posed by online environments.

INOBTR.org (I Know Better) is a public outreach organization that focuses on helping keep kids safe on and offline through community and public awareness efforts. The organization has worked in conjunction with DOJ on various national public awareness campaigns such as Project Safe Childhood. Project Safe Childhood is a unified and comprehensive strategy to combat child exploitation, which combines law enforcement efforts, community action and public awareness. The organization has also developed large-scale public awareness events, such as Child Cyber Safety Night at the Ballpark to educate on child cyber safety. See featured Project Safe Childhood videos at http://www.justice.gov/psc/videos. For more information about INOBTR, visit www.inobtr.org.

C) Please indicate specific actions that your country will undertake as a follow-up

The U.S. will continue its outreach efforts to educate the public about online safety through its own initiatives and grant funding to non-governmental organizations.

Operational Goal: Share best practices among Global Alliance countries for effective strategies to inform the public about the risks posed by online, self-exploitative conduct in order to reduce the production of new child pornography.

A) ***Please report on implementation of any measures announced in your country's 2013 report***

See below.

B) ***Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance***

The U.S.'s online safety outreach efforts, including videos and guides, are posted online and available to other Global Alliance countries. See information reported in above operational goal.

C) ***Please indicate specific actions that your country will undertake as a follow-up***

The U.S. will continue its online safety outreach efforts and ensure that any related products are available online. During its leadership of the Global Alliance, the U.S. plans to facilitate the continuing exchange of best practices among Global Alliance countries, and to secure participation of new Global Alliance members who can learn from these best practices.

Policy Target No. 4

Reducing as much as possible the availability of child pornography online and reducing as much as possible the re-victimization of children whose sexual abuse is depicted.

Operational Goal: Encourage participation by the private sector in identifying and removing known child pornography material located in the relevant State, including increasing as much as possible the volume of system data examined for child pornography images.

A) ***Please report on implementation of any measures announced in your country's 2013 report***

See below.

B) ***Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance***

More than 3.2 million reports of suspected child sexual exploitation (including child pornography) have been made to NCMEC's CyberTipline between 1998 and December 2014. The CyberTipline alerts law enforcement to possible child sexual exploitation in their jurisdiction and maximizes the limited resources available in the fight against child sexual abuse. Increasingly, the value of the CyberTipline as a source of leads for law enforcement has been greatly enhanced by collaboration with internet service providers in the private sector. During the normal course of business, many online companies voluntarily search their systems to ensure that they are not inadvertently hosting online child pornography. In 2014, NCMEC launched the Industry Hash Sharing Platform, which allows participating online companies to share their own company-created list of hash values and PhotoDNA signatures associated with child sexual abuse images. This is a voluntary, industry-only platform that is designed to facilitate the sharing of information between online companies seeking to reduce the amount of child sexual exploitation material on their servers.

Under the UK/US Taskforce to Counter Online Child Exploitation (see Policy Target No. 1, *supra),* two working groups comprised of members of the private sector are working on the following concepts, which are specifically directed at removing child pornography material from circulation: (1) Device-level Blocking of Known Child Sexual Abuse Images. Through a global database of hashes or signatures of known child pornography images, device-level blocking could be used to automatically restrict the download, upload, and sharing of known images; and (2) Anonymous Self-reporting of Indecent Imagery. Provide children with an anonymous self-

report facility to allow children to anonymously inform industry when they have disseminated an indecent, self-generated image so that industry can blacklist the image. Industry could then prevent the further distribution of such images and disrupt offenders' efforts to use the images to blackmail children.

C) Please indicate specific actions that your country will undertake as a_ follow-up

DOJ will continue to support the WePROTECT working groups in their efforts to implement the developed concepts. In 2015, NCMEC will be launching an NGO Hash Sharing Platform that will allow global, non-government organizations to share their own created list of hash values and PhotoDNA signatures associated with child sexual abuse images. This is a voluntary program designed to facilitate the sharing of multiple hash lists with participating organizations seeking to reduce the amount of child sexual exploitation material on their servers.

Operational Goal: Increase the speed of notice and takedown procedures as much as possible without jeopardizing criminal investigation.

A) ***Please report on implementation of any measures announced in your country's 2013 report_***

See below.

B) ***Please assess progress made in your country to pursue this shared policy target and to reach this operational goal of the Global Alliance***

NCMEC is actively engaged in "notice and takedown" measures. Since 2010, under its Notice Tracking Initiative, NCMEC has sent thousands of notices about URLs containing apparent child pornography to the relevant domestic or international hosting provider, and those companies may use the information to enforce their terms of service. In 2014, the average time for the provider to take down the content is 26 hours after NCMEC notification. Each year, the takedown rate has improved significantly.

C) Please indicate specific actions that will be undertaken as a follow-up

DOJ will continue to provide funding to NCMEC to support its notice and takedown measures, and any other initiatives that will result in the reduction of the availability of child pornography online.