Australia

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
Actions ALREADY UNDERTAKEN	
Description of the actions already undertaken	• Under Australia's Constitution, responsibility for combating child sexual exploitation is shared between the Commonwealth and States and Territories. The States and Territories are responsible for child sex-related offences occurring domestically, while the Commonwealth can create offences where there is an international element to the crime or where the offences are committed online or through the postal service. • The Australian Government has acted strongly to combat child pornography in areas within its jurisdiction. In the Criminal Code Act 1995, the Australian Government has enacted laws against: o dealing in child pornography and child abuse material overseas o using a carriage or postal service for child pornography or child abuse material, for example viewing a child pornography video online or sending a child pornography image through the mail, and o possessing, producing, supplying or obtaining child pornography or child abuse material for use through a carriage or postal service. • These offences carry penalties of up to 15 years imprisonment, with higher penalties of up to 25 years imprisonment applying to aggravated offences. Aggravated offences apply to those who offend on multiple occasions along with other offenders as part of a child pornography network. • Specific defences to Australia's child pornography laws are available to law enforcement, intelligence or security officers acting in the course of their duties if their conduct is reasonable in the circumstances for the purpose of performing that duty. This is important to facilitate child pornography investigations, as it allows law enforcement officers to send child sexual exploitation material to their colleagues for the purpose of investigation, without committing an offence. • In 2010, minor consequential amendments were also made to Australia's laws to ensure that existing law enforcement powers were available to combat all child sex-related offences. • Since December 2010, the Australian Federal Police (AFP) have been uploading images and data into ICSE, including victims identified by all Australian Police Services.

	• Two Australian police forces (AFP and Queensland Police) have dedicated Victim Identification Teams, whilst the other Australian law enforcement agencies include this role within their broader Child Protection areas. • The Australian New Zealand Police Advisory Agency Child Protection Working Group (ANZPAA CPWG) consists of representatives from all Australian police forces and New Zealand Police. The charter for ANZPAA CPWG is to identify, develop, review and co-ordinate police practices, policy and procedures in relation to all aspects of child protection. • Use of the AFP International Liaison Officer network to facilitate the cooperation between Australian and International law enforcement. This network is utilised to identify and provide capacity building to foreign law enforcement. • Secondment of police officers between both domestic and international law enforcement agencies. For example, an FBI agent was seconded to the AFP's Child Protection Operations for 6 months, and there has been an exchange of members between AFP and New South Wales and Victoria Police. • The AFP is facilitating research assistance to a number of studies examining the underlying factors relating to the self-generation of child pornography material, and related factors.
Actions that WILL BE UNDERTAKEN	
Description of the actions that <u>will be undertaken</u> and timeframe	• Deployment of a national data base that will assist law enforcement agencies manage, search, share and analyse evidence (predominantly imagery) in child exploitation cases across law enforcement agencies. This database will exchange data with ICSE. • Additional exchange or secondment of specialised officers between law enforcement agencies. • Further capacity building (both resources and training) for law enforcement agencies overseas, with emphasis on identified Child Sex Tourism (CST) destination countries.

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
Operational Goal:	Improve the joint efforts of law enforcement authorities across Global Alliance countries to investigate and prosecute child sexual abuse online
Actions ALREADY UNDERTAKEN	
Description of the actions already undertaken	• Australia (AFP) is a member of the Virtual Global Taskforce (VGT), an international law enforcement alliance to combat online exploitation of children with the aim of creating a safer online environment. • Liaison with industry and development of a solution enabling the timely provision of key investigative information through the establishment of agreements. This has negated the use of Mutual Assistance Requests which were unable to provide the information in a timely fashion. • Consequently the AFP is working with Australian Attorney-General's Department to streamline the mutual assistance process aimed at shorter turnaround times. • The AFP (High Tech Crime Operations) has a team dedicated to a crime prevention role relating to both child online safety and wider cybercrime awareness. This team runs an ongoing education program named ThinkUknow, which focuses on raising awareness of online risks amongst parents, carers and teachers. • The AFP has also participated in joint international investigations. • The Cybersmart.gov.au website provides comprehensive, up-to-date and age appropriate advice and educational resources, aimed at parents, teachers and children. The site has attracted over 2.3 million visitors since its launch. • Professional Development (PD) program given to educators to provide them with the skills, resources and confidence to assist young people enjoy safe and positive online experiences. Over 12,000 teachers have attended the PD program and over 670,000 students, parents and teachers have attended presentations/workshops offered by Cybersmart since Jan 2009.
Actions that WILL BE UNDERTAKEN	
Description of the actions that will be undertaken and timeframe	• AFP participation in joint international investigations which arise during the period. • Ongoing review and development of Cybersmart resources, including website enhancements and mobile portal, outreach through social media channels and professional development programs. New cybersafety program for 8 – 12 year olds for roll-out in 2014. • Publication of new research into young people's use of online social media, including risks they face and strategies for managing these risks – due mid-2013.

	• Roll out of revised Professional Development program that is customized by schools to better meet their needs.

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
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
Actions ALREADY UNDERTAKEN	
Description of the actions already undertaken	• Through the AFP's Cyber Crime Prevention Team, a number of resources have been developed to assist in raising awareness of online risks. These resources are tailored for youth as well as parents, carers and teachers through the ThinkUKnow cyber-safety program. • The resources are available for downloading from the following sites: http://www.afp.gov.au/policing/cybercrime/crime-prevention.aspx http://www.thinkuknow.org.au/ • The resources for parents, carers and teachers are available in languages other than English.
Actions that WILL BE UNDERTAKEN	
Description of the actions that will be undertaken and timeframe	• As the need arises, the AFP will be updating its educational cyber-safety collateral to ensure it responds to the changing risks of the online environment.

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.
Operational Goal:	Increase the speed of notice and takedown procedures as much as possible without jeopardizing criminal investigation
Actions ALREADY UNDERTAKEN	
Description of the actions <u>already undertaken</u>	• In conjunction with a number of Australian Internet Service Providers, the AFP are blocking websites known to contain child pornography by utilising the Interpol 'Worst of' list. • The AFP is also co-operating with private industry on developing/improving technology enabling the filtering of P2P traffic for known child pornography. • The Broadcasting Services Act 1992 (Cth) (the BSA) establishes a co-regulatory scheme for dealing with online content. The law places specific responsibilities on government and industry to ensure rapid take-down of child abuse material, without compromising criminal investigations. • Schedule 7 to the BSA sets out clear legal procedures for the takedown of child abuse material hosted within Australia by the Australia Communications and Media Authority (ACMA), including penalties for non-compliance with a take-down direction. This is supported by codes of practice developed by the Internet industry, and registered by the ACMA, which set out procedures for ISPs in dealing with takedown directions. • In investigating complaints received from members of the public, the ACMA adheres to international best practice by prioritising taking action on all reports of online child abuse material within 48 hours of first receiving a report. • Under Schedule 7 to the BSA, the ACMA must notify child abuse material hosted in Australia to the relevant state or territory police for investigation. The ACMA defers taking any further action until advised by the force concerned that doing so will not prejudice criminal investigations. These relationships are underpinned by memorandums of understanding (MOUs) between the ACMA and the states and territories. • An MOU between the ACMA and the AFP enables the ACMA's involvement in the international system for notification and takedown of child abuse material that operates under the auspices of the International Association of Internet Hotlines (INHOPE). The MOU allows the ACMA to report overseas hosted child sexual abuse material (and other illegal content) to either the AFP or through INHOPE for law enforcement attention and take down in the host country OR a country where the content has been produced. This

	arrangement is authorised under schedules 5 and 7 to the BSA, and was revised and strengthened in January 2013. • Liaison between law enforcement agencies, the ACMA and the Internet industry is frequent and actively pursued by all parties, ensuring collaborative and productive relationships. • The Telecommunication Act 1997 (Cth) (the Telco Act) places obligations on the ACMA to assist police in preventing criminal offences. The Telco Act also requires carriers and carriage service providers to give help to state, territory or commonwealth authorities in enforcing criminal laws.
Actions that WILL BE UNDERTAKEN	
Description of the actions that <u>will be undertaken</u> and timeframe	• The AFP will expand the number of Australian Internet Service Providers which block websites using the Interpol 'Worst of' list. • Final testing and deployment of technology to filter P2P traffic. • The ACMA is investigating systems that would facilitate the transmission of information/data collected in relation to specific child abuse images to law enforcement agencies. • New MOUs between the ACMA and the states and territories will be drafted, incorporating the additional flexibility in referring material that was built into the 2013 MOU between the ACMA and the AFP. • Research and adopt technologies that will facilitate the investigation of online content, particularly in relation to P2P, mobile and TOR distributed material, is actively undertaken and shared with law enforcement agencies and other INHOPE hotlines.