Australian Government
Attorney-General's Department

National Plan to Combat Cybercrime

ACHIEVING A JUST AND SECURE SOCIETY | www.ag.gov.au

MINISTER'S FOREWORD

Digital technologies and the internet have transformed our everyday lives. We use them to access information, conduct business, keep in touch with family and friends, and engage with Government. The internet offers huge potential for our country.

But with greater openness, interconnection and dependency comes greater risk. Our use of the internet has created new opportunities for financially motivated cyber criminals and those who seek to target vulnerable members of our community.

Organised criminal groups are increasingly using digital technologies to facilitate their illegal activities, to commit both traditional crimes such as theft and fraud and also new crimes enabled by advancing technologies.

Australian governments recognise the serious threat posed by cybercriminals and are working together to combat this threat as part of a collaborative national response. The National Plan to Combat Cybercrime provides a consistent strategic direction for agencies involved in this response.

The Plan represents a national commitment to ensuring a safer and more secure digital environment for all Australians. It identifies key principles that will underpin our approach, and key priorities to strengthen our national response.

As a key initiative under the Plan, the Australian Cybercrime Online Reporting Network (ACORN) will make it easier for the public to report cybercrime, get the information they need to protect themselves and ensure agencies can respond more quickly. The ACORN will also give a clearer picture of the scope and nature of cybercrime affecting Australians and enable better operational and policy responses.

Importantly, combating cybercrime requires more than just an enforcement response—prevention, mitigation and education are important aspects. It is also a shared responsibility—between individuals, industry and governments. No one can combat this threat alone.

The Plan entrenches these notions in a framework that will unify efforts across jurisdictions and form a key plank of the Government's broader digital agenda.

The Hon Mark Dreyfus QC, MP
Attorney-General of Australia

ISBN 978-1-922032-18-8

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Business and Information Law Branch
Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Call: 02 6141 6666
Email: copyright@ag.gov.au

CONTENTS

Foreword 1

Contents 3

Introduction 4

A National Plan to Combat Cybercrime 6

Implementing the Plan 7

Key principles underpinning our approach 7

Key priorities for government action 8

Key priority—Educating the community to protect themselves 10

Key priority—Partnering with industry to tackle the shared problem of cybercrime 12

Key priority—Fostering an intelligence-led approach and sharing information 14

Key priority—Improving the capacity and capability of agencies to address cybercrime 16

Key Priority—Improving international cooperation on cybercrime 18

Key priority—Ensuring the criminal justice framework is effective 20

Appendix A: Roles and responsibilities 24

Appendix B: Summary of initiatives 27

INTRODUCTION

The internet and digital technologies are bringing many benefits to Australians. Increasing connectivity allows us to stay in touch with family and friends, access services and communicate and create online. Australia has more than 12 million internet subscribers and a further 17.3 million mobile handset subscribers;[1] while over 11 million Australians have a Facebook account.[2] The National Broadband Network is increasing the opportunities for Australians to participate in a growing global digital economy.

However, just as the internet and other new technologies are opening up tremendous possibilities, they also provide opportunities for criminals to commit new crimes and to carry out old crimes in new ways.

The nature of the problem

On the evidence available, it is clear that the number, sophistication and impact of cybercrimes continues to grow and poses a serious and evolving threat to Australian individuals, businesses and governments.

Although it is difficult to quantify the total costs, evidence from operational agencies suggests that economic costs of cybercrime in Australia are substantial. As many instances of cybercrime go unreported, it is difficult to give an accurate figure. However, non-government estimates put the cost of cybercrime in Australia as high as $2 billion annually.[3]

And there are other costs of cybercrime that cannot be quantified—no dollar value can reflect the harm caused to victims by the distribution of child exploitation material or the compromise of personal information, or the emotional hardship of being left financially destitute.

Online, criminals can commit crimes across multiple borders in an instant and can target a large number of victims simultaneously. Tools that have many legitimate uses, like high speed internet, peer to peer filesharing and sophisticated encryption methods, can also help criminals to carry out and conceal their activities. Despite these challenges, cybercrime is still a form of crime and requires a long term, sustained response from Australian governments.

What is cybercrime?

In Australia, the term 'cybercrime' is used to describe both:

- crimes directed at computers or other information communications technologies (ICTs) (such as hacking and denial of service attacks), and
- crimes where computers or ICTs are an integral part of an offence (such as online fraud, identity theft and the distribution of child exploitation material).[4]

The first category consists of offences which only exist in the digital world, such as criminals hacking networks to steal sensitive business information or attacks against websites to extort money or by 'hacktivists'.

1 http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0
2 http://www.socialmedianews.com.au/social-media-statistics-australia-june-2012/
3 Norton Cybercrime Report 2012.
4 This definition is taken from the Protocol for Law Enforcement Agencies on Cybercrime Investigations developed by the National Cybercrime Working Group.

The second category covers old crimes committed in new ways. The internet and digital technologies provide a platform for committing crimes such as fraud and identity theft on an industrial scale. Our increased connectivity has created new opportunities for criminals, new methods of delivery and new 'business models', bringing the online forms of these crimes within the definition of cybercrime.

The anonymity and reach of the internet can also magnify antisocial behaviours which exist in the offline world, such as bullying and harassment. While not all instances of this behaviour are criminal, sufficiently serious instances may be treated as such.

For the purposes of this Plan, the term 'cybercrime' does not include instances where the use of the internet or technology is merely incidental to a crime (for example, a drug importation organised via email). While these crimes fall outside the above definition, their investigation often requires the same technical skills, investigative powers and international cooperation arrangements as cybercrime. To this extent, the initiatives in this Plan will help to improve the ability of our agencies to respond to them.

The current response

A range of government agencies are involved in responding to different aspects of cybercrime in Australia. Under current arrangements, State and Territory agencies have primary responsibility for cybercrime that targets individuals, businesses and government systems in their jurisdictions. Commonwealth agencies have primary responsibility for cybercrime directed at critical infrastructure, systems of national interest and Commonwealth Government systems.[5]

The National Cybercrime Working Group (NCWG) brings together representatives from State, Territory and Commonwealth law enforcement and justice agencies to ensure that agency efforts in response to cybercrime are properly aligned.

Other agencies involved in responding to cybercrime include consumer protection agencies and offices of fair trading (responsible for online scams) as well as national security and intelligence agencies (responsible for the threat posed to government networks by malicious cyber actors), including through the multi-agency Cyber Security Operations Centre (CSOC) in the Department of Defence.[6] Australia's national computer emergency response team, CERT Australia, provides the initial point of contact for industry for cyber security incidents impacting upon Australian networks. The roles and responsibilities of agencies involved in responding to cybercrime are described in more detail at **Appendix A**.

5 *Protocol for Law Enforcement Agencies on Cybercrime Investigations.*

6 The CSOC comprises representatives from Defence, Australian Federal Police, CERT Australia and the Australian Security Intelligence Organisation.

A NATIONAL PLAN TO COMBAT CYBERCRIME

Australian governments recognise that the challenge presented by cybercrime is one that requires a coordinated national response.

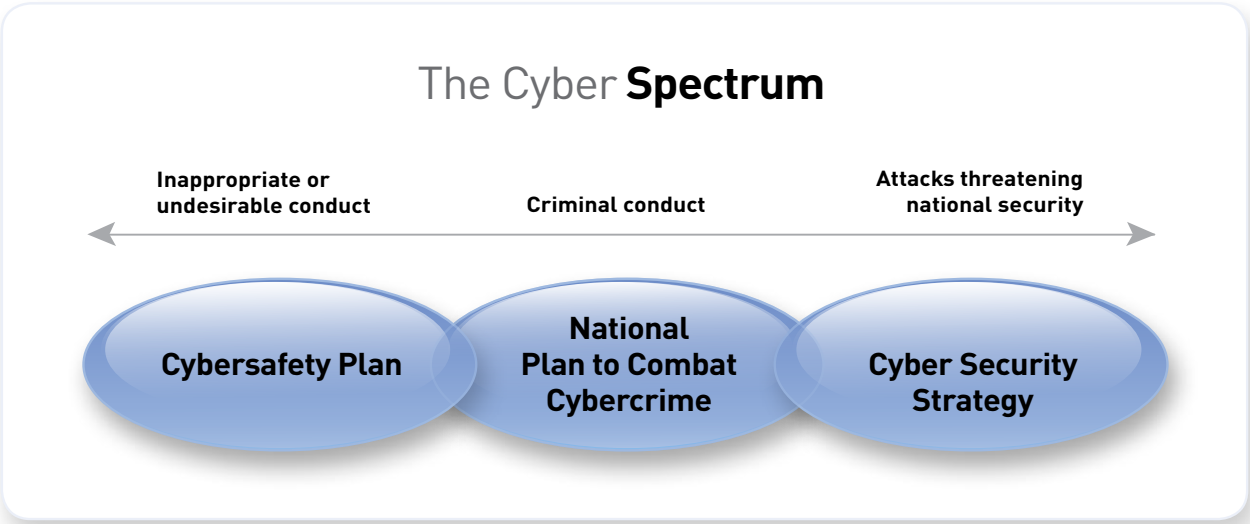
This Plan represents a commitment from the Commonwealth, State and Territory governments of Australia to work together to address the threat of cybercrime.

While the Plan focuses on the steps that governments will take, it also acknowledges the key roles played by industry and individuals and the importance of forging strong partnerships to deal with cybercrime.

The Plan sets out key principles and priority areas of focus over the short to medium term, outlining what we will achieve and how we will achieve it. It identifies initiatives and reflects on existing efforts in Australia's response to cybercrime.

Our vision is for a safe and secure digital environment for all Australians.
We will achieve this by making Australia a hard target for cyber criminals.

Cybercrimes are part of a spectrum of conduct that ranges from activities which are undesirable or inappropriate at one end—not all of which are criminal—through to activities which could constitute threats to national security at the other. This Plan focuses on the centre of this spectrum.



The Commonwealth Government's Cybersafety Plan focuses on the broader social and personal risks associated with the use of computers and the internet and the protection of children online. The Commonwealth's Cyber Security Strategy outlines the vision for a secure, resilient and trusted cyber environment, and provides a framework to better address threats to computer systems and data, including those systems which underpin our national security, critical infrastructure and systems of national interest.

This Plan integrates with these existing strategies, recognising that in many cases, the best way to protect against cybersafety or security risks is also the most effective way of protecting against cybercrime.

The Cybercrime Plan also supports a range of other Commonwealth Government strategies, including the National Security Strategy, National Digital Economy Strategy, Organised Crime Strategic Framework and National Organised Crime Response Plan and National Identity Security Strategy. It also supports and promotes the development of State and Territory strategies to respond to cybercrime.

IMPLEMENTING THE PLAN

The NCWG will be responsible for coordinating and implementing Australia's national response to cybercrime as outlined in this Plan. While this Plan outlines steps to improve our response in the short to medium term, the changing nature of cybercrime requires a flexible and evolving response.

To ensure that our actions take account of emerging issues, the NCWG will provide an annual update to the Standing Council on Law and Justice and the Standing Council on Police and Emergency Management on the national response to cybercrime. The NCWG's update will track the implementation of the initiatives outlined in this Plan and identify opportunities to enhance our response as new trends and technologies emerge.

KEY PRINCIPLES UNDERPINNING OUR APPROACH

Four key principles support our national approach to cybercrime. These principles form the underlying philosophy of our national response to cybercrime.

1. Understanding the problem

Having a better understanding of how cybercrime affects Australia will help us address it—we need to know who it targets and why, how it targets them, who the perpetrators are and how much harm it is causing. Armed with this information, governments can better shape policy responses and allocate resources, and businesses and individuals can better assess risk and take targeted action to protect themselves.

2. Partnerships and shared responsibility

Tackling cybercrime is, and always will be, a shared responsibility between individuals, industry and government. This means forging mutually beneficial partnerships to share information and combine efforts to combat cybercrime. Governments will also explore other partnership arrangements, including with overseas law enforcement agencies and with key industry sectors, such as internet service providers (ISPs), online service providers and the tertiary education sector.

3. Focusing on prevention

Australian governments recognise that it is better to prevent cybercrime from happening than to respond to it after it has occurred. In many cases, effective preventative measures are relatively low cost and easy to implement. Users need to take steps to avoid falling victim to cybercrime and governments and industry need to be proactive in anticipating where new threats might emerge.

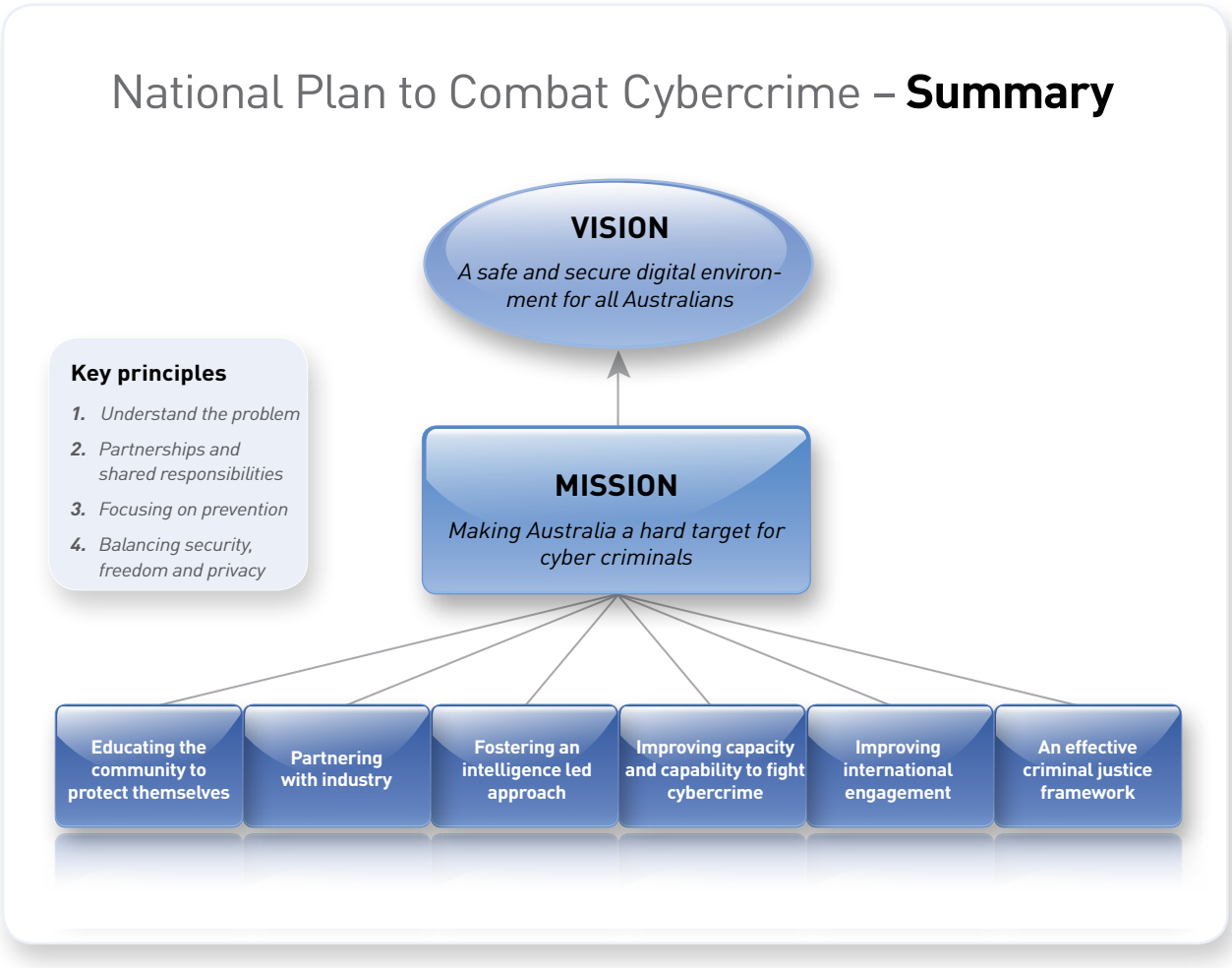
4. Balancing security, freedom and privacy

The internet is built upon the freedom, creativity and innovation of users. In striving to create a more secure online environment and take action against cyber criminals, our response must balance the rights of Australians to freely roam, create and interact on the internet, and uphold individuals' right to privacy.

KEY PRIORITIES FOR GOVERNMENT ACTION

Governments have identified six priority areas for action shaped around the critical contributions governments can make in strengthening our national response to cybercrime—areas where we must focus our efforts for the short to medium term in building our response to cybercrime:

- educating the community to protect themselves
- partnering with industry to tackle the shared problem of cybercrime
- fostering an intelligence-led approach and information sharing
- improving the capacity and capability of government agencies, particularly law enforcement, to address cybercrime
- improving international engagement on cybercrime and contributing to global efforts to combat cybercrime and
- ensuring an effective criminal justice framework.



KEY PRIORITIES

KEY PRIORITY—EDUCATING THE COMMUNITY TO PROTECT THEMSELVES

As with crime in the physical world, no amount of action by governments and the private sector can prevent every cybercrime. Those of us who use digital technologies have to take responsibility for our own security and safety online and exercise safe online practices.

Most instances of financially-motivated cybercrime can be prevented by taking simple steps or by knowing what to look out for. Governments and industry can assist users to understand these steps and to recognise the warning signs.

We aim to ensure all Australians are aware of the risks of cybercrime, can take steps to protect themselves and know where they can get help if they fall victim to cybercrime.
To achieve this, we will focus our efforts on getting our message out to users and making it easier to report cybercrime.

Getting our message out to users

Commonwealth, State and Territory governments all provide advice on safe internet practices to assist users to take steps to protect themselves online through initiatives such as www.staysmartonline.gov.au, www.cybersmart.gov.au, www.scamwatch.gov.au, National Cyber Security Awareness Week and the AFP's ThinkUKnow cybersafety program, as well as through publications like Protecting Yourself Online, Protecting Your Identity and the Easy Guide to Socialising Online.

Australian governments will continue to work together to provide up-to-date advice to businesses and the community on safe online practices and will develop mechanisms to assess the effectiveness of these efforts.

- At the Commonwealth level, the Department of Broadband, Communication and the Digital Economy (DBCDE) plays a key role in education and awareness-raising about cybersafety and security risks.
- At the national level, the NCWG will work to ensure coordination of cybercrime messaging across jurisdictions.

The private sector also plays a key role in promoting safe online practices with their clients and customers. In particular, financial institutions, ISPs and e-commerce services account for millions of online transactions and client relationships.

Australian governments will continue to work closely with these sectors, and develop partnerships to spread advice to clients about protecting themselves from cybercrime. Governments will also encourage businesses to adopt practices aimed at promoting secure online behaviour throughout the wider community, including the distribution of effective and low cost tools for preventing and detecting online threats.

The Commonwealth Government is also partnering with the community and the private sector to promote the concept of responsible digital citizenship to ensure that Australian users are able to not only protect themselves online, but also positively contribute to the development of an innovative, dynamic and civil online culture. This work is being led by the Australian Communications and Media Authority, which is developing a set of best practice principles along with tools and guidance for putting these into practical effect.

Making it easier to report cybercrime

Those who fall victim to cybercrime need to know where to report it and get assistance. The uncertainty about how and where to report can deter victims from reporting, limiting our ability to respond to and understand cybercrime. A recent UN study of cybercrime found that cybercrimes most frequently come to the attention of law enforcement authorities through reports from victims but that very few victims ever make a report.

Key initiative: The Australian Cybercrime Online Reporting Network

Australian governments have committed to establishing a national online reporting facility for cybercrime—the Australian Cybercrime Online Reporting Network (ACORN). The ACORN will provide access to general educational advice, and refer reports to law enforcement and government agencies for further consideration and investigation where appropriate. The NCWG will oversee the development and implementation of the ACORN.

The ACORN will help to address several of the key priorities identified in this plan. In particular, it will:

- **reduce confusion around how to report cybercrime**. As there are many agencies across the Commonwealth, States and Territories which play a role in investigating cybercrimes, there can be a lack of clarity for victims about how and where different types of cybercrime should be reported
- **provide centralised aggregated data on cybercrime in Australia** and improve our understanding of its scope and total cost, supplementing the current intelligence picture of cybercrime and informing policy and operational responses to cybercrime
- **streamline the process of referring cybercrime reports between law enforcement and other relevant government agencies**, minimising law enforcement resources occupied in redirecting cybercrime reports to the most appropriate agency, and
- **provide a centralised point for advice on avoiding cybercrime**, to provide up to date advice to businesses and the community.

KEY PRIORITY—PARTNERING WITH INDUSTRY TO TACKLE THE SHARED PROBLEM OF CYBERCRIME

The private sector has a key role in making Australia a harder target for cybercrime. As commerce and services migrate online, business networks will pose increasingly attractive targets for cyber criminals. As owners and operators of the systems and practices that support the digital economy, the private sector is well placed to take responsibility for its own protection and to assist clients to do the same.

Governments will work closely with industry to respond to the shared problem of cybercrime—by providing education and resources, jointly developing effective regulatory frameworks and sharing actionable information and intelligence.

Australian governments will work in close partnership with business and industry to respond to the shared problem of cybercrime and to promote a safer and more secure digital environment for Australians.

Empowering businesses to look after themselves

Governments have developed resources for industry and business on the steps they can take to protect themselves and their clients from cybercrime. Examples of this include:

- The Stay Smart Online website managed by DBCDE, which provides information and advice to small and medium enterprises on the steps they can take to protect themselves and their customers online.
- The Australian Signals Directorate's Top 35 Strategies to Mitigate Targeted Cyber Intrusions. The CSOC estimates that at least 85% of cyber intrusion techniques could be mitigated by implementing the top four mitigation strategies.
- CERT Australia's work in providing actionable cyber threat information to Australian businesses to assist them to make informed decisions about risk.
- The Australian Government's Protective Security Policy Framework, which provides a risk management model for how Government agencies protect their people, information and assets. This framework provides an effective model which can readily be adopted by business and industry.

Australian governments will also support industry-led arrangements to counter online threats. For example, the Australian Government is working with Australia's four largest banks to develop mechanisms to share information and strengthen the financial and banking industry response to fraud through the National Fraud Exchange Initiative.

To encourage the private sector to act in the interest of the online community, Australian governments will continue to promote the development of frameworks such as the iCode, which provides a framework for ISPs to implement measures to protect their customers and their networks.

The Commonwealth Government has also introduced a Bill in the Commonwealth Parliament to amend the *Privacy Act 1988* to create a mandatory requirement for companies and government agencies to report data breaches. Such a scheme would enable affected individuals to take action to lessen the adverse effects of personal information becoming compromised. It could also help to provide more accurate empirical data on the extent of the problem in Australia while promoting the adoption of strengthened data security practices by companies and government agencies. The proposed laws are based on feedback received from a discussion paper circulated in October 2012. If enacted, the laws will commence in March 2014.

In addition, Australian governments will support research and initiatives to 'design out' cybercrime—to consider how products and services can be designed to become more difficult to exploit for criminal purposes—in order to assist business to minimise the opportunities available to criminals to exploit the online environment.

As an initial step, Australian governments will consider the application to cybercrime of work being undertaken by the Australian Institute of Criminology in the context of broader crime prevention to look at ways to support this type of approach. The NCWG will also explore other ways in which Australian governments can support efforts to 'design out' cybercrime.

Cooperation with industry

Key industries—such as ISPs, software and hardware companies—have a particularly close connection with digital technologies and services. Some possess sophisticated capabilities to analyse the digital environment and are well placed to assist in proactively identifying emerging cybercrime trends.

Governments will continue to explore options for enhanced public/private information sharing on cybercrime, and for cooperation on mutually-beneficial research and development initiatives designed at better understanding and minimising cybercrime.

The Commonwealth will continue to encourage more businesses to report instances of cybercrime to CERT Australia to get direct practical support to deal with issues they face.

A key function of the Australian Cyber Security Centre (discussed further below) will be to ensure Australian networks are among the hardest to compromise in the world. In doing so, it will work closely with critical infrastructure sectors and key industry partners to protect our nation's most valuable networks and systems. The Centre will also provide advice and support to develop preventative strategies to counter cyber threats.

KEY PRIORITY—FOSTERING AN INTELLIGENCE-LED APPROACH AND SHARING INFORMATION

Criminals are quick to find ways to exploit new technologies to further their illicit activities. Agencies must stay up-to-date with these methods so that they can recognise emerging trends, patterns and problem areas. Sharing quality, timely and comprehensive information and intelligence—between law enforcement agencies, intelligence agencies and the private sector—will lead to a better understanding of cybercrime and more effective responses. This will occur in a privacy-protective way, in accordance with legislative frameworks and with effective oversight.

We aim to develop an enhanced intelligence picture of the cybercrime threat facing Australia.
To achieve this, we will focus our efforts on gathering intelligence from the public, business and government agencies and undertaking mutually beneficial information exchanges with the private sector.

Cybercrime intelligence

To inform this Plan, the Australian Crime Commission (ACC) worked with agencies involved in combating cybercrime to produce a national assessment of the scope and scale of the cybercrime facing Australia, and a collection plan to support future assessments. This assessment provides a criminal intelligence snapshot of cybercrime in Australia in 2013.

The Assessment provides a good starting point for governments to make better informed decisions and to allocate resources based on current trends and problem areas. However, as cybercrime is an evolving threat, it will be necessary to regularly refresh our understanding.

The ACC will provide an annual update on cybercrime to help ensure that agencies' efforts under the Plan are appropriate to the current threat environment. A version of this will be made publicly available where possible. In addition, agencies will look for opportunities to provide cybercrime intelligence to the ACC's National Criminal Intelligence Fusion Centre to supplement the real time national picture of the threat of serious and organised crime in Australia.

The ACORN will also help us to develop a better understanding of cybercrime in Australia by providing a centralised national online facility for members of the public to report cybercrime—who it affects, how and what can be done about it, what patterns of behaviour might exist and trends affecting Australia. Data from the ACORN will also feed into the ACC's National Criminal Intelligence Fusion Centre.

The development of an Australian Cyber Security Centre will also provide opportunities to sharpen our understanding of cybercrime.

The Australian Cyber Security Centre

On 24 January 2013, the Prime Minister announced that the Commonwealth would establish the Australian Cyber Security Centre (ACSC), which will bring together the Government's most sophisticated cyber security capabilities in a single facility. This will be a considerable step in making Australia a harder target for malicious cyber activities, including cybercrime.

The ACSC will enable a more complete understanding of threats across the cyber spectrum and facilitate faster and more effective responses to serious cyber incidents. It will promote more seamless interaction between governments, industry and international partners.

The Commonwealth will explore ways to build the cybercrime intelligence picture through the ACSC, with a priority on strengthening collaboration with industry and State and Territory partners

Work is underway to improve information sharing more broadly between and within governments. At the Commonwealth level, the National Security Information Environment Roadmap sets out the strategy for more effective information sharing within the federal national security community, including on cybercrime. Nationally, the Australia New Zealand Policing Advisory Agency (ANZPAA) e-Crime Working Group (AeCWG) provides a forum for sharing technical information and specialist knowledge on cybercrime. The AeCWG is exploring options to improve sharing operational information between agencies, including through ACORN.

Often, data on offences does not distinguish between offences committed online and those committed offline. To further assist in developing a better picture of cybercrime, Australian police agencies will work towards common standards for recording cybercrimes.

Information sharing with the private sector

Businesses are often the first to become aware of emerging cybercrime threats and are also best placed to protect themselves against them. Information sharing arrangements between businesses and governments must be robust and effective. While there are sound policy reasons for certain barriers to information sharing—including privacy, commercial and national security concerns—these must be balanced with the importance of sharing information to support our collective efforts to address the cybercrime challenge.

To improve our collective understanding of the cybercrime threat environment, Australian governments will explore options to enhance the two-way flow of information between government agencies and the private sector where appropriate.

Australian governments have already taken steps to achieve this. CERT Australia works with private sector partners to assist them in protecting their computer systems, and to share information on cyber incidents and threats. This is complemented by relationships between industry and the agencies represented in the CSOC as well as ASIO's Business Liaison Unit. The Trusted Information Sharing Network for Critical Infrastructure Protection also provides an environment where business and government can share information to protect our critical infrastructure and ensure the continuity of essential services in the face of all hazards.

KEY PRIORITY—IMPROVING THE CAPACITY AND CAPABILITY OF AGENCIES TO ADDRESS CYBERCRIME

The rapid pace and cross-border nature of cybercrime pose challenges for traditional regulatory and law enforcement approaches. In order to generate the strongest possible response to cybercrime, we need to go beyond traditional law enforcement activities and explore options to predict, prevent and disrupt online criminal activity.

We aim to ensure that our agencies have the capabilities and capacity to respond to cybercrime and to address unnecessary barriers to effective cooperation in response to cybercrime, both domestically and internationally.
To achieve this, we will focus on improving the coordination of our responses and addressing identified capability and capacity gaps within agencies.

Domestic coordination

The borderless nature of cybercrime means that no single Australian jurisdiction can effectively tackle cybercrime in isolation. It requires a cooperative approach.

Australian governments already have in place mechanisms to help ensure effective cooperation and coordination in responding to cybercrime issues, including:

- the NCWG, which was established by the Standing Council on Law and Justice and involves police and justice representatives from all jurisdictions, and
- the AeCWG and Electronic Evidence Specialist Advisory Group (EESAG), which allow for collaboration between Australian cybercrime investigators and digital evidence specialists.

One product of this collaboration is the *Protocol for Law Enforcement on Cybercrime Investigations* (the Protocol), which was developed in 2011 by the AeCWG and the NCWG. The Protocol provides a simple way to identify the most appropriate agency to deal with a cybercrime matter, taking into account the different kinds of cybercrimes, the nature and location of victims and offenders and a number of other contextual factors.

The NCWG will oversee a regular review of the Protocol to ensure that it continues to provide an effective means of coordinating cybercrime investigation activity.

The ACORN will also be invaluable for coordinating agency efforts. When established, the ACORN will automatically refer reports of cybercrime it receives from members of the public to the most appropriate agency, based initially on the arrangements set out in the Protocol. In doing so, it will reduce the resources currently used by agencies in manually referring the cybercrime reports they receive to the most appropriate agency for action.

Capacity and capabilities

The capacity and capabilities of our agencies, particularly law enforcement agencies, need to keep pace with evolving technologies if police are to perform their duties in the digital environment.

At the most basic level, all police officers need to know how to gather and analyse digital evidence, leaving specialist units to focus on more complex cybercrimes. Specialist units within law enforcement agencies must have the training and capabilities to detect and investigate the more complex and sophisticated use of technology in criminal activities.

Recognising the significant overlap between investigating cybercrimes and analysing digital evidence, the AeCWG and EESAG have developed training and education guidelines for technology crime investigators and digital evidence specialists. The guidelines provide a benchmark for skills development and national consistency in technology crime and digital evidence capabilities. The AeCWG has also undertaken an assessment of law enforcement cybercrime capabilities and is working to implement priority recommendations from the assessment.

The NCWG will encourage basic training on cybercrime and digital evidence becoming a mainstream component of police training, including by continuing to support the development of nationally consistent training and education resources and continued monitoring of capability gaps.

Recruiting and retaining people with the appropriate skills is an essential component of ensuring our agencies are ready to deal with the cybercrime challenge.

The NCWG will consider options to:

- increase the pool of knowledge at law enforcement's disposal, including by examining options to leverage the expertise of the private and tertiary sectors, and
- coordinate access to specialist expertise across our police forces, including through the development of a national centre of excellence or an agreement about the sharing of specialist resources across Australian police agencies.

Powers

In addition to the technical capacity required, law enforcement and national security agencies need effective powers to investigate cybercrimes. These powers must keep track with the evolving nature of modern technologies and criminal methodologies.

The NCWG will monitor law enforcement powers which relate to the investigation of cybercrime and the collection of digital evidence to ensure they remain effective.

Given the key role telecommunication interception techniques play in this area, the Commonwealth Government referred a discussion paper to the Parliamentary Joint Committee on Intelligence and Security on options to modernise the telecommunication interception regime. The Committee reported on 24 June 2013. The Committee's report recognises the need for Australia's agencies to have the necessary powers to carry out their work, and notes that intrusive powers must be balanced by appropriate privacy safeguards. The report recommends a comprehensive revision of the interception regime, in consultation with interested stakeholders.

KEY PRIORITY—IMPROVING INTERNATIONAL COOPERATION ON CYBERCRIME

The interconnectivity of the internet means that Australia's geographical remoteness is no barrier to foreign criminals who want to target Australian victims. Our agencies can face significant challenges in bringing cyber criminals in other countries to justice. Cybercrime is an international problem which requires a coordinated and cooperative international response.

We aim to identify and minimise barriers to swift and effective international cooperation in response to cybercrime. To achieve this, we will promote harmonised legal frameworks internationally and assist other countries to build their capacity to respond to cybercrime. We will also work with international partners to improve cooperation on cybercrime.

Harmonised legal frameworks and capacity building

Differences in national laws and the capacity of local agencies to enforce those laws can create a barrier to effective international cooperation on cybercrime. Savvy cyber criminals can exploit these inconsistencies by operating in countries with weak laws or enforcement regimes. We can improve this situation by encouraging as many countries as possible to strengthen and harmonise their domestic legislation on cybercrime and supporting them to build enforcement capacity.

Australia has acceded to the *Council of Europe Convention on Cybercrime* (the Cybercrime Convention). The Convention provides a comprehensive model framework of offences and law enforcement powers and facilitates close cooperation between member countries. It has become the cornerstone of a harmonised approach to cybercrime for a growing global community of nations.

The Commonwealth Government will engage internationally to promote effective global response to cybercrime. In particular, the Commonwealth will encourage other countries to adopt the Cybercrime Convention as a basis for national cybercrime laws to foster greater international cooperation.

Capacity building in the Pacific

The Commonwealth Attorney-General's Department, under the Pacific Police Development Program, provides capacity building assistance to Pacific Island countries to strengthen crime and policing laws. As part of this assistance, we—with partner countries—review cybercrime offences in the context of broader criminal justice legislation review projects in the Pacific. For example, AGD is working with Nauru and the Cook Islands to review and reform their criminal laws, including cybercrime laws, and has worked with Samoa to review proposed cybercrime offences.

We also support regional capacity building initiatives to address cybercrime. In April 2011, AGD jointly hosted a cybercrime legislation workshop with the Secretariat of the Pacific Community and the Council of Europe in Tonga. This workshop provided Pacific island countries with international best practice to assist with development of domestic cybercrime legislation consistent, as far as possible, with the Cybercrime Convention.

As countries within our region develop better and more extensive digital infrastructure, the Commonwealth Government will continue to assist in building their capacity to combat cybercrime. Australia is a key contributor to international and regional organisations and forums which are committed to facilitating cooperative relationships in combating cybercrime, so bringing together both developed and developing countries from across the globe. The Commonwealth Government will participate in these forums to promote effective global responses to cybercrime and to help countries build their capacity to deal with cybercrime.

Cooperation with key allies

Australian governments recognise that the global nature of cybercrime means that our agencies must collaborate with overseas partners to target those who seek to exploit the internet for criminal gains. As a highly developed country, Australia is well placed to make a significant positive contribution to the global fight against cybercrime. We can also learn from overseas counterparts to improve our national response.

The Quintet of Attorneys General, comprising Attorneys General from Australia, Canada, New Zealand, the United Kingdom and United States, is considering ways to streamline cooperation on cybercrime. In 2011, Attorneys General agreed to an action plan to combat cybercrime in recognition of the common challenge our nations share in combating this key global threat.

As part of the action plan, it was agreed that countries would scope the ability to link online reporting facilities in Quintet countries to one another, in order to improve our collective understanding of cybercrime. Once the ACORN is established, Australian governments will consider options to share information collected through the ACORN with similar facilities in other countries.

Depending on the country from which material is sought, the type of material which is sought and the legislative requirements in the country from which material is sought, formal mutual assistance procedures may be required in order to obtain certain foreign assistance. Seeking evidence through these procedures may take significant time—which can be at odds with the speed with which cyber criminals act and the ease with which digital evidence can be destroyed. In these circumstances, informal assistance mechanisms including agency-to-agency cooperation are encouraged in the first instance to ensure formal mutual assistance requests can be actioned as quickly as possible. Such mechanisms need to balance privacy and security concerns and be subject to appropriate privacy oversight mechanisms.

Australia participates in the 24/7 global network of high tech crime points of contact under the Cybercrime Convention, which allows for speedy assistance between signatory countries. Australian law enforcement agencies also maintain their own networks with counterparts around the world, such as through the Strategic Alliance Cyber Crime Working Group.

To improve our international cooperation, the NCWG will develop a protocol to clarify and guide international engagement by Australian law enforcement agencies. This will highlight the importance of informal police to police arrangements and identify channels for agencies to seek investigational assistance and pass investigation-related information to other countries.

CERT Australia has also developed relationships with other national CERTs and international CERT groupings in response to global cyber threats, such as botnets, distributed denial-of-service attacks and malware. These relationships can be used to request practical assistance, for example in taking down botnet controllers targeting computers in Australia.

KEY PRIORITY—ENSURING THE CRIMINAL JUSTICE FRAMEWORK IS EFFECTIVE

Australia's criminal justice system must provide an effective framework for investigation and prosecution of cybercrime. This means that offences must account for the use of new and emerging technologies to commit crime; penalties must provide adequate deterrent and reflect the seriousness of different types of cybercrime; procedural and evidentiary rules need to account for new forms of evidence; and prosecutors and judicial officers must be well equipped to consider digital evidence.

In addition to facilitating the investigation and prosecution of criminal conduct, the criminal law also plays an important normative role in shaping society's acceptance or non-acceptance of different forms of behaviour. For this reason also, criminal laws need to continue to reflect society's views by appropriately criminalising malicious online conduct and provide mechanisms for its punishment.

We aim to ensure Australia's criminal justice system provides an effective framework for investigating and prosecuting cybercrime and deterring would-be cyber criminals and that Australian courts, judicial officers and legal practitioners have the capacity to deal with cybercrime and digital evidence.

Effective criminal offence frameworks

At the Commonwealth level, offences in the *Criminal Code Act 1995* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) cover crimes directed at computers and ICTs, such as unauthorised access and distributed denial of service attacks. These offences are based on model provisions agreed to by all jurisdictions. The Criminal Code also includes offences for the misuse of telecommunications services for criminal purposes, such as the online distribution of child exploitation material. These offence provisions are supported by a range of powers which can be exercised by law enforcement and national security agencies in the detection, disruption and investigation of those offences.

Each State and Territory also has offences for crimes directed at computers and ICTs that stand alongside the Commonwealth offences. Critically, States and Territories have primary responsibility for laws dealing with online versions of personal and property crimes, such as stalking, theft and fraud. Each State and Territory also maintains the legal framework for its agencies to detect, disrupt and investigate offences.

While Australia's current legal frameworks effectively cover the range of conduct that constitutes cybercrime, it is important that new technologies do not allow criminals to exploit loopholes.

The NCWG will continue to monitor the existing offence and penalty frameworks in Australian jurisdictions to ensure the law remains effective in light of technological advancements. In its annual update to Ministers, the NCWG will identify the need for changes to existing legislation to deal with emerging threats and technologies.

Assisting prosecutors and the judiciary to deal with cybercrime and digital evidence

Prosecution of cybercrime offences is an important part of the enforcement framework to deal with cybercrime and assists in creating and maintaining public confidence in our criminal justice system.

In order for cybercrime offences to be prosecuted effectively, prosecutors and judicial officers need to be able to understand and evaluate technical digital evidence. While courts and the legal profession are becoming more accustomed to the use of new technology to commit crime, the admission of digital evidence can still be a technical process. As the use of technology in crime grows, prosecutors and judges will increasingly be required to present and understand highly technical details in order to effectively administer the law.

Governments can continue to assist prosecutors and the judiciary by providing the resources they need to respond to legal concepts associated with new technology and the facilities they need to analyse and consider digital evidence in a court setting.

The Australian Federal Police has been proactive in providing training workshops for the legal community and developing mechanisms to improve the presentation of digital evidence in courts, particularly through the development of the eCourt facility.

The Commonwealth Director of Public Prosecutions has produced a Cybercrime Manual which provides guidance for investigators and prosecutors on Commonwealth cybercrime offences, including an analysis of the elements that need to be proved to make out an offence, draft charges and other important information such as the commencement of the offence, the penalty and any definitions, and information on various technologies used in committing cybercrime.

Australian governments support these initiatives and, through the NCWG, will investigate further ways to make it easier for legal practitioners and courts to handle digital evidence.

APPENDICES

APPENDIX A: ROLES AND RESPONSIBILITIES

The Commonwealth **Attorney-General's Department (AGD)** is responsible for Commonwealth criminal law policy (including cybercrime), identity security, protective security, privacy, critical infrastructure resilience and telecommunications interception policy, each of which is a key element in protecting the national security of an increasingly digitally enabled Australia. The Secretary of AGD chairs the National Cybercrime Working Group, which comprises representatives from Commonwealth, State and Territory police and justice agencies. AGD works to build the capacity of partner countries, especially in the Pacific region, to better respond to instances of cybercrime by assisting in the reform of these countries' criminal justice and policing legislation. AGD is also responsible for making and receiving formal mutual assistance requests to and from foreign countries to seek or provide evidence to support cybercrime investigations or prosecutions.

AGD has responsibility for **CERT Australia**, which provides the initial point of contact for industry for cyber security incidents impacting upon Australian networks. CERT Australia also works with government and industry partners to ensure that all Australians and Australian businesses have access to information on how to better protect their information technology environment from cyber-based threats and vulnerabilities.

The **Australian Communications and Media Authority (ACMA)** is responsible for the regulation of broadcasting, the internet, radio communications and telecommunications. It is responsible for leading the whole-of-government awareness-raising efforts aimed at promoting responsible digital citizenship through the development of the Digital Citizenship Best Practice Principles. The ACMA contributes to the development of a safer online environment through notifying ISPs of malware infections identified among their customers, anti-spam work and administration of a frontline complaints mechanism for reports about illegal online content, including child sexual abuse material. It also operates the Cybersmart program, a national cyber education program aimed at educating young people, parents and teachers about skills and behaviours necessary to create positive and safe online experiences.

The **Australian Competition and Consumer Commission (ACCC)** is an independent statutory authority responsible for encouraging competition and fair trade in the online marketplace to benefit consumers, business and the community. The ACCC's primary responsibility is to ensure that individuals and businesses comply with the Commonwealth's competition, fair trading and consumer protection laws. The ACCC conducts educational campaigns and outreach activities to raise awareness of consumers' rights and responsibilities, including in the online environment. In addition, the ACCC works to disrupt identified scam activities and, where appropriate, prosecute offenders for breaches of the *Competition and Consumer Act 2010* (Cth), including the Australian Consumer Law. The ACCC maintains the ScamWatch.gov.au website which provides advice and a facility for reporting scams that increasingly operate in the online environment.

The **Australian Crime Commission (ACC)** is Australia's national criminal intelligence agency. It is a statutory authority with unique investigative capabilities which it draws on to provide government with an independent view of the risk of serious and organised crime. The ACC maintains national criminal intelligence holdings; produces strategic intelligence assessments; and coordinates national operational responses to disrupt, disable and prevent organised crime impacting on Australia.

The **Australian Federal Police (AFP)** is responsible for enforcing federal criminal law and protecting national interests from crime in Australia and overseas. The AFP's High Tech Crime Operations portfolio provides the AFP with an enhanced capability to investigate, disrupt and prosecute offenders committing serious and complex cybercrimes. These include significant computer intrusions such as distributed denial of service attacks and breaches of major computer systems. The AFP plays a role in raising awareness of cyber risks through its ThinkUKnow program delivering internet safety training to parents, carers and teachers.

The **Australian Security Intelligence Organisation (ASIO)** is making Australia a hard target for malicious cyber activity by gathering and producing intelligence that enables it to warn the Government about activities or situations that might endanger Australia's national security. ASIO investigates cyber activity conducted for the purpose of espionage, sabotage, terrorism or other forms of politically motivated violence, and contributes to the investigation of computer network operations directed against Australia's systems.

The **Australia New Zealand Policing Advisory Agency (ANZPAA)** is a joint initiative of the Australian and New Zealand Police Ministers and Commissioners. ANZPAA provides strategic and policy advice on policing regarding cross-jurisdictional issues to enhance community safety and security. The ANZPAA Crime Forum's e-Crime Working Group (AeCWG) brings together senior jurisdictional ecrime representatives for co-ordination and information sharing purposes, as well as policy and strategy development. The Electronic Evidence Specialist Advisory Group (EESAG), a group formed by the Senior Managers of Australia New Zealand Forensic Laboratories, provides for the coordination and sharing of technical information and specialist knowledge among the wider community, including policing, which is focused on improving the response to e-crime.

The **Commonwealth Director of Public Prosecutions (CDPP)** is responsible for the prosecution of Commonwealth criminal offences including Commonwealth offences involving cybercrime. The CDPP has considerable experience in the prosecution of cybercrime offences and maintains the Cybercrime Manual for prosecutors and investigative agencies which provides guidance in relation to cybercrime offences and other information relevant to the investigation and prosecution of cybercrime offences. In addition the CDPP maintains manuals dealing with search warrants, telephone intercepts and surveillance devices that assist investigators in the investigation of cybercrime and other offences.

CrimTrac is an Executive Agency responsible for the development and maintenance of national information sharing systems between State, Territory and Commonwealth law enforcement agencies. Through the convergence of common information services, the development of innovative interoperable capabilities and enhancements to national police data holdings, CrimTrac will contribute directly to the effectiveness and efficiency of law enforcement agencies in Australia and their ability to combat cybercrime.

The **Department of Broadband, Communications and the Digital Economy (DBCDE)** is responsible for creating an environment that supports Australians taking full advantage of the opportunities of the digital economy. DBCDE promotes measures to assist Australians and Australian businesses to take up online opportunities, ensures all Australians can access internet services, and empowers consumers to operate safely and securely online through its education and awareness-raising initiatives and activities, such as National Cyber Security Awareness Week and the Cybersafety Help Button.

The **Department of Defence's Cyber Security Operations Centre (CSOC)**, a multi-agency body run by the Australian Signals Directorate, has two main roles. The first is to provide Government with a better understanding of sophisticated cyber threats against Australian interests. The CSOC identifies malicious activity conducted by sophisticated foreign hackers by using advanced analytic capabilities and techniques. The CSOC also provides advice and assistance regarding cyber events across the Australian government. CSOC staff work with external government agencies to improve the security stance of their networks. They also work with agencies whose networks have been compromised to help mitigate further cyber intrusions.

The **Department of Finance and Deregulation's Australian Government Information Management Office (AGIMO)** works across government to maintain Australia's position as a leader in the productive application of information and communications technologies (ICT) to government administration, information and services. AGIMO fosters the efficient and effective use of ICT by Australian government departments and agencies. It achieves these aims by developing whole of government ICT policies to meet emerging trends, analysing significant government ICT proposals (including assessing the adequacy of agencies' cyber security provisions and risks), providing practical guidance to agencies, delivering programs to develop ICT skills and supporting ICT governance bodies.

The **Department of Foreign Affairs and Trade (DFAT)**, in consultation with relevant agencies, advances and protects Australia's interests in relation to combating cybercrime internationally, including meeting our international legal obligations. Staff at Australia's overseas diplomatic missions represent Australia in relevant international and multilateral fora, engaging organisations such as the United Nations Office on Drugs and Crime in Vienna. DFAT is also actively engaged at the regional level on cybercrime and related issues, including in the ASEAN Regional Forum. DFAT staff also facilitate and represent Australia in bilateral discussions with other countries on cybercrime.

The **Department of the Prime Minister and Cabinet (PM&C)** is responsible for Commonwealth whole-of-government coordination and leadership for cyber policy issues and chairs the Cyber Policy Group. PM&C is also the lead policy agency for cyber security, working closely with operational agencies to ensure that the government has a coordinated response to cyber risks and opportunities. PM&C leads the government's international engagement policy on cyber issues. PM&C also leads work undertaken by the national security community under the National Security Information Environment Roadmap to enhance Australia's information management environment.

The **Office of the Australian Information Commissioner (OAIC)** is Australia's national privacy and freedom of information regulator. The OAIC also provides advice to the Australian Government on government information policy. Under the *Privacy Act 1988*, the OAIC regulates the handling of personal information by Australian, ACT and Norfolk Island government agencies and private sector organisations covered by the Act, including obligations relating to the security of personal information. In this context, the OAIC works with agencies and the private sector to encourage the adoption of best privacy practices.

State and Territory law and justice agencies are responsible for criminal law policy, police and emergency management policy, and courts and corrective services in their jurisdictions. Similarly, State and Territory Directors of Public Prosecution are responsible for the prosecution of offences under the laws of their jurisdictions.

State and Territory police cybercrime units are responsible for the development of preventative initiatives and investigation of all cyber offences committed against the person, business, and state, territory and local government. This includes offences directed against computing and communication technologies as well as offences where the use of the internet or information technology is integral to the commission of the offence such as computer fraud, electronic payment fraud, the dissemination of online child exploitation material and data theft.

APPENDIX B: SUMMARY OF INITIATIVES

Priority	Desired outcomes	Actions/initiatives
Educating the community to protect themselves	**All Australians are aware of the risks of cybercrime, can take steps to protect themselves, and know where they can get help if they fall victim to cybercrime.**	All Australian Governments will work together to: • **implement a national online reporting facility for cybercrime—the ACORN—**to provide Australians with a national point-of-contact to receive reports of cybercrime, provide access to general educational advice, and refer reports to law enforcement and government agencies for further consideration and possible investigation where appropriate. • **provide up-to-date advice to businesses and the community** on safe internet practices and how to avoid falling victim to cybercrime and will develop mechanisms to assess the effectiveness of these efforts. ◦ At the Commonwealth level, DBCDE plays a key role in cyber security and safety education and awareness raising efforts. ◦ The NCWG will work to ensure national consistency of messaging relating to cybercrime across agencies in all Australian jurisdictions. ◦ The ACMA will facilitate the coordination of awareness raising initiatives relating to digital citizenship, including developing digital citizenship best practice guidance, to ensure a forward-focused approach to informing citizens about their rights and responsibilities. ◦ Governments will continue to work closely with industry on education and awareness raising efforts - particularly key sectors such as internet service providers, the financial sector and ecommerce service providers. • **encourage businesses to adopt practices aimed at promoting secure online behaviour throughout the wider community,** such as the distribution of effective and low cost tools for the prevention and detection of online threats.

Priority	Desired outcomes	Actions/initiatives
Partnering with industry to tackle the shared problem of cybercrime	**Close partnerships with business and industry to respond to the shared problem of cybercrime and to promote a safer and more secure digital environment for Australians**	To develop closer partnerships with industry on cybercrime, all Australian governments will work together to: • encourage **industry-led arrangements to protect against and minimise the impact of cybercrime** on Australian businesses and their clients, including through the development of self-regulatory frameworks. • **explore options to increase information-sharing with industry** on cyber threats and vulnerabilities for **enhanced public/private information sharing on cybercrime,** and for **cooperation on mutually-beneficial research and development initiatives** designed at better understanding and minimising cybercrime, including by involving law enforcement and other agencies in CERT Australia's regular national information exchanges. • **support research and initiatives to 'design out' cybercrime** to assist business in minimising the opportunities available to criminals to exploit the online environment. • **encourage more businesses to report instances of cybercrime to CERT Australia** to provide an accurate and current picture of the cybercrime threat to business and get direct practical support to deal with issues they face. The Commonwealth Government will: • work with Australia's major banks to **establish a National Fraud Exchange between Australia's key financial institutions.** • promote the Protective Security Policy Framework as a model for business and industry to protect their information. • **introduce mandatory data breach notification laws.** • **continue to notify ISPs of malware infections** identified among their customers under the Australian Internet Security Initiative.

Priority	Desired outcomes	Actions/initiatives
Fostering an intelligence-led approach and information sharing	**A better informed national response to cybercrime through an enhanced intelligence picture of the threat facing Australia.**	To improve the criminal intelligence picture on cybercrime, Australian governments will: • consider **an annual update from the Australian Crime Commission on the nature, scale and impact of cybercrime,** taking into account key developments since the previous assessment. • **collate cybercrime intelligence from across Australia and provide it to the Australian Crime Commission Fusion Centre** to supplement the real time national picture of the threat of serious and organised crime in Australia. • **ensure the Australian Cybercrime Online Reporting Network has the capacity to aggregate data on cybercrime reports it receives,** which will improve our understanding of the scope and cost of, and prevailing trends in, cybercrime. • **explore other innovative ways to improve our understanding of cybercrime,** including through the use of 'big data', while being sensitive to the associated privacy concerns. • **explore options to enhance the two-way flow of information between government agencies and the private sector where appropriate,** including through CERT Australia's national information exchanges, ASIO's Business Liaison Unit, the Trusted Information Sharing Network and the ACC's information sharing powers • explore options to **build the cybercrime intelligence picture through the Australia Cyber Security Centre,** including options to improve collaboration with industry and State and Territory law enforcement agencies. Law enforcement agencies in all jurisdictions will: • implement procedures to **enhance the ability to identify where reported crimes are cybercrimes work towards common standards for recording cybercrimes.**

Priority	Desired outcomes	Actions/initiatives
Improving the capacity and capability of government agencies, particularly law enforcement, to address cybercrime	**Government agencies, particularly law enforcement agencies, have the capabilities and capacity they need to detect, disrupt, investigate and prosecute cybercrime and manage digital evidence.** **No unnecessary barriers to timely and effective cooperation in response to cybercrime, both domestically and internationally.**	To strengthen domestic coordination of law enforcement, all Australian governments, through the National Cybercrime Working Group, will: • **oversee a regular review of the** Protocol for Law Enforcement on Cybercrime Investigations to ensure clears lines of responsibility for different types of cybercrime and to enhance the management of cross-jurisdictional cybercrime offences. • ensure the **Australian Cybercrime Online Reporting Network has the capacity to refer reports to the law enforcement agency in the most appropriate jurisdiction.** • continue to **explore other mechanisms to improve cooperation on cybercrime matters across Australian jurisdictions** through the National Cybercrime Working Group and the ANZPAA e-Crime Working Group. To ensure law enforcement agencies have the capacity and capabilities to investigate cybercrime, the National Cybercrime Working Group will: • encourage basic training on **cybercrime and digital evidence becoming a mainstream component of police training,** including by continuing to support the development of nationally consistent training and education resources. • consider options to **increase the pool of knowledge at law enforcement agencies' disposal,** including options for accessing expertise from the private and tertiary sectors, such as through secondments. • consider options to **coordinate access to specialist expertise across our police forces,** including through options for a national centre of excellence or an agreement about the sharing of specialist resources across Australian police agencies. • continue to **monitor capability gaps across our police forces** to guide capability improvement. • **monitor law enforcement powers which relate to the investigation of cybercrime and collection of digital evidence** to ensure they remain effective.

Priority	Desired outcomes	Actions/initiatives
Improving international engagement on cybercrime	**Barriers to swift and effective international cooperation in response to cybercrime are identified and minimised.**	To ensure effective international cooperation on cybercrime, the Australian Government will: • **promote the Council of Europe Convention on Cybercrime** as the global standard for harmonised legal frameworks on cybercrime. • **continue to assist countries in the region to build their capacity to combat cybercrime** and to bring their laws into line with global best practices. • **implement the Quintet action plan on cybercrime** and explore further ways to streamline arrangements for cooperation between likeminded countries on cybercrime investigations. • **support Australian agencies participating in worldwide cybercrime response efforts,** including ◦ the **'24/7 network' of cybercrime investigators,** encouraging other countries to join the network to improve timely international police assistance in cybercrime matters, and ◦ **international networks dedicated to law enforcement notification and take-down of illegal online content,** such as the Australian Communications and Media Authority's involvement in the International Association of Internet Hotlines (INHOPE). The National Cybercrime Working Group will: • develop **a protocol to clarify and guide international engagement** by Australian law enforcement agencies.

Priority	Desired outcomes	Actions/initiatives
Ensuring the criminal justice framework is effective	**Australia's criminal justice system provides an effective framework for investigating and prosecuting cybercrime and deterring would be cyber criminals.** **Australian Courts, judicial officers and legal practitioners have the capacity to deal with cybercrime and digital evidence.**	To ensure the criminal justice system continues to keep pace with technological change, the National Cybercrime Working Group will: • **monitor offences and their penalties** to ensure the law remains effective in light of technological advancements. • as part of the annual update to the Standing Councils on Law and Justice and Police and Emergency Management, **identify the need for changes to existing legislation** to deal with emerging threats and technologies. • investigate further ways to **make it easier for legal practitioners and courts to handle digital evidence** as confidently and expeditiously as other forms of evidence.