Australian Government

# CYBER SECURITY STRATEGY

# MINISTER'S FOREWORD

Australians have been quick to embrace the Internet in their lives and businesses. For most of us it is now part of our daily routine for talking to our friends and family, studying, shopping and paying bills. Equally, business has adopted the Internet and other information technology to improve efficiency, improve the quality of service and gain access to new markets.

Unfortunately our use of the Internet has also created new opportunities for criminals who seek to access our personal and corporate secrets, steal our resources and intimidate Internet dependent businesses. The Prime Minister in his 2008 National Security Statement to Parliament acknowledged that online threats now form one of our top tier national security priorities.

Organised crime is increasingly employing information and communication technologies to facilitate their illegal activities, particularly in relation to money laundering and identity crime.

This Strategy shows how the Australian Government is harnessing the full range of resources to help protect government, business and individual Australians. It describes how new capabilities have been created to help Australians, and the businesses they transact with, be better protected.

Importantly, this Strategy calls upon all Australian Internet users to be vigilant and informed about online threats and how their own actions can be the first line of defence.

The Hon Robert McClelland MP
Attorney-General

ISBN: 978-1-921241-99-4

# Table of Contents

# EXECUTIVE SUMMARY

The Prime Minister has indicated that cyber security is now one of Australia's top tier national security priorities. The global community continues to experience an increase in the scale, sophistication and successful perpetration of cyber crime. As the quantity and value of electronic information has increased so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying out their activities.

Australia's national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (ICT). This includes desktop computers, the Internet, mobile communications devices and other computer systems and networks.

## A more insidious and damaging threat

The production, sale and distribution of malicious code has become a prolific criminal industry, making malware stealthier, more targeted, multi-faceted and harder to analyse and defeat. The risk to the Australian economy from computer intrusion and the spread of malicious code by organised crime has been assessed as high. This is particularly the case for financial transactions and sensitive commercial or personal identity information.

There is a growing array of state and non-state actors who are compromising, stealing, changing or destroying information and therefore potentially causing critical disruptions to Australian systems. The distinction between traditional threat actors – hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services – is increasingly blurred. With the borderless, anonymous nature of the Internet, attribution of the source of attacks is difficult.

## A government-led coherent, integrated approach

Confronting and managing these risks must be balanced against the civil liberties of Australians, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy.

The aim of the Australian Government's cyber security policy is the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy.

While the Australian Government's cyber security policy is primarily concerned with the availability, integrity and confidentiality of Australia's ICT, it must be coordinated with those of other related policies and programs such as cyber *safety* which is focused on helping to protect individuals, especially children, from exposure to illegal and offensive content, cyber-bullying, stalking, and grooming online for the purposes of sexual exploitation.

## Guiding principles

Consistent with the enduring principles outlined in the Prime Minister's National Security Statement, the Australian Government's cyber security policy is based on the following guiding principles:

***National leadership:*** The scale and complexity of the cyber security challenge requires strong national leadership.

***Shared responsibilities:*** All users, in enjoying the benefits of ICT, should take reasonable steps to secure their own systems, exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users.

***Partnerships:*** In light of these shared responsibilities, a partnership approach to cyber security across all Australian governments, the private sector and the broader Australian community is essential.

***Active international engagement:*** Given the transnational nature of the Internet, in which effective cyber security requires coordinated global action, Australia must adopt an active, multi-layered approach to international engagement on cyber security.

***Risk management:*** In a globalised world where all Internet-connected systems are potentially vulnerable and where cyber attacks are difficult to detect, there is no such thing as absolute cyber security. Australia must therefore apply a risk-based approach to assessing, prioritising and resourcing cyber security activities.

***Protecting Australian values:*** Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms. Maintaining this balance is a continuing challenge for all modern democracies seeking to meet the complex cyber security challenges of the future.

## Objectives

The objectives of the Australian Government's cyber security policy are that:

- All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online.
- Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers.
- The Australian Government ensures its information and communications technologies are secure and resilient.

## Strategic priorities

To achieve these objectives the Australian Government applies the following strategic priorities to its programs:

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest.
- Educate and empower all Australians with the information, confidence and practical tools to protect themselves online.
- Partner with business to promote security and resilience in infrastructure, networks, products and services.
- Model best practice in the protection of government ICT systems, including the systems of those transacting with government online.
- Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests.
- Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber crime.
- Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

## New capabilities

Integral to the Australian Government's Cyber Security Strategy are two new mutually supporting organisations: CERT Australia and the Cyber Security Operations Centre (CSOC).

The Australian Government is bringing together Australia's national computer emergency response team (CERT) arrangements into a new body, CERT Australia. CERT Australia will be the national coordination point within the Australian Government for the provision of cyber security information and advice for the Australian community, and be the official point of contact in the expanding global community of national CERTs to support more effective international cooperation.

Established as an initiative of the Australian Government's Defence White Paper, the CSOC provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance. The CSOC will identify and analyse sophisticated cyber attacks, and assist in responses to cyber events across government and critical private sector systems and infrastructure.

These new initiatives will build on existing Australian Government cyber security capabilities.

## Conclusion

With the rapid escalation in the intensity and sophistication of cyber crime and other cyber security threats, it is imperative that government, business and the community are aware of the severity of cyber security risks, and commit to work together to protect what has become a vital component of our economy and society.

# INTRODUCTION

> *…the sophistication of our modern community is a source of vulnerability in itself …. we are highly dependent on computer and information technology to drive critical industries such as aviation; electricity and water supply; banking and finance; and telecommunications networks. This dependency on information technology makes us potentially vulnerable to cyber attacks that may disrupt the information that increasingly lubricates our economy and system of government.*
>
> The Hon Kevin Rudd MP, Prime Minister of Australia

The Australian Government acknowledges the scale of the cyber security challenge, which the Prime Minister has indicated is now one of Australia's top tier national security priorities. Australia's national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (ICT). This includes desktop computers, the Internet, mobile communications devices and other computer systems and networks. As these technologies become more pervasive in our lives, government, business and individuals are becoming more dependent upon them for a variety of purposes and functions, ranging from online purchases of goods and services (including government services), communicating with others, searching for information and managing finances through to controlling equipment in the mining and manufacturing industries. Computers and computer-based communications are ubiquitous in Australian life. Sometimes these uses are quite clear to see and understand – whereas in other cases, such as the control of utilities, transport and hospital equipment or the supply of food and pharmaceuticals, the extent of dependence on ICT is not as obvious.

The Australian Government recognises the importance and benefits of the advances in technology to Australia's digital economy. The Australian Government has established a new company to invest up to $43 billion over eight years to build and operate a National Broadband Network (NBN) to deliver superfast broadband access for all Australians. The NBN represents the single largest investment in broadband infrastructure in Australia's history and will further transform the way Australians communicate and do business.

### The Digital Economy

The Australian Government has outlined its vision for Australia's digital economy in the report *Australia's Digital Economy: Future Directions*.

The digital economy is the global network of economic and social activities that are enabled by platforms such as the Internet, mobile and sensor networks. A successful digital economy is essential for Australia's economic growth and our ability to maintain our international standing. The digital economy is highly dynamic. It will ultimately encompass the entire economy and many, if not all, aspects of our society.

The key elements that a successful digital economy in Australia will encompass are:

- a digitally aware and enabling Government
- a digitally confident, innovative and skilled industry, and
- a digitally literate and empowered community.

Effective cyber security is a critical enabler to the Australian Government's goal of maximising opportunities for all Australians to benefit from the digital economy.

The global community continues to experience an increase in the scale, sophistication and successful perpetration of cyber crime. As the quantity and value of electronic information has increased so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying out their activities.

**The financial loss from computer security events against Australian businesses during the 2006-07 financial year is estimated by the Australian Institute of Criminology to be between $595 and $649 million.[1] Given the tendency for much cyber crime to be under reported, this could be a significant underestimate.**

Just as we have seen the benefits of ICT in promoting legitimate economic activity, we now see cyber crime emerging on an unprecedented scale. The emergence of an underground cyber crime 'industry' means that it is no longer necessary to possess technical skills to commit cyber crime. An underground economy has developed where criminal capabilities, techniques and tools can be readily purchased or hired on a commercial basis. These extend from compromised credit card details or even complete identities and tools to create malicious software (malware) through to the ability to hire networks of compromised computers (botnets) to undertake tasks such as spamming, hosting offensive content and distributed denial of service (DDoS) attacks.

[1] K Richards, *The Australian business assessment of computer user security: a national survey*, Australian Institute of Criminology, 2009.

**Antivirus vendor Symantec identified that malicious code signatures had increased globally by 265 percent between 2007 and 2008. Sixty per cent of all malware detected by Symantec to date was detected in 2008 alone.[2]**

The production, sale and distribution of malicious code has become a prolific criminal industry, making malware stealthier, more targeted, multi-faceted and harder to analyse and defeat. The risk to the Australian economy from computer intrusion and the spread of malicious code by organised crime has been assessed as high. This is particularly the case for financial transactions and sensitive commercial or personal identity information.

Attacks on critical computer systems in both the government and private sector are being contemplated as an alternative way of conducting warfare and a means by which criminals, terrorist groups and hostile intelligence services could damage Australia's national interests. For example, malicious activities against ICT systems have caused the disruption of electric power systems in multiple regions overseas, including a case that resulted in a major multi-city power outage.[3]

**According to antivirus vendor Trend Micro, Australian computers experienced 17,692,567 malware infections in 2008. Australia reported the fifth highest level of infections worldwide.[4]**

Some recent DDoS attacks have resulted in the degradation and complete disruption of online services in Australia, impacting systems that are critical to Australia's national interest, such as the financial sector. Such attacks are inexpensive to conduct, potentially hugely destructive and can be instigated from almost anywhere in the world.

There is a growing array of state and non-state actors who are compromising, stealing, changing or destroying information and therefore potentially causing critical disruptions to Australian systems. The distinction between traditional threat actors – hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services – increasingly appears to be blurring. With the borderless, anonymous nature of the Internet, attribution of the source of attacks is difficult.

The speed of technological change associated with next generation networks is challenging traditional notions of what constitutes computer networks and how we should secure them. This includes the combination of increased bandwidth; convergent voice, data, video networks; mobile wireless devices; embedded processors and sensors; social networking and other Web 2.0 applications; and Internet-based networks (cloud computing).

---

2 Symantec Corporation, *Symantec global Internet security threat report - trends for 200*8, Volume XIV, April 2009.

3 *United States Cyberspace policy review - assuring a trusted and resilient information and communications infrastructure*, 2009 < http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

4 Trend Micro, *Trend Micro 2008 annual threat roundup and 2009 forecast*, 2008.

The only prediction that can be made with any confidence is that modern ICT will continue to evolve in ways not foreseen by its designers and that it will be used for malicious as well as legitimate purposes.

These factors, combined with the global nature of the Internet and the limitations in the direct influence of governments over modern ICT networks that are predominantly designed, built, owned and operated by the private sector, serve to emphasise the complexity of the cyber security challenge facing Australia in the twenty-first century.

### National Security Statement

On 4 December 2008, the Prime Minister delivered Australia's inaugural National Security Statement to the Parliament. The Statement outlines five enduring national security interests that constitute the Australian Government's national security objectives:

- maintaining Australia's territorial and border integrity
- promoting Australia's political sovereignty
- preserving a cohesive and resilient society and strong economy
- protecting Australians and Australian interests both at home and abroad, and
- promoting a stable, peaceful and prosperous international environment, particularly in the Asia Pacific region, together with a global rules-based order which enhances Australia's national interests.

The Statement indicates electronic espionage, both commercial and state-based, will be a growing vulnerability as the Australian Government and society become more dependent on integrated information technologies. It states that this challenge must and will be met with full vigour and identifies cyber security as amongst the Australian Government's top tier national security priorities.

Australia is vulnerable to the loss of economic competitiveness through the continued exploitation of ICT networks and the compromise of intellectual property and other sensitive commercial data. This has the potential to undermine Australians' confidence in the digital economy. Cyber security is therefore not just an issue of national security but also one of economic security.

It is a challenge that requires a coherent, integrated approach – led by government, but working in close partnership with the private sector – that seeks to address the strategic vulnerabilities of an increasingly hostile online environment. Confronting and managing these risks must be balanced against the civil liberties of Australians, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy.

# THE AUSTRALIAN GOVERNMENT APPROACH TO CYBER SECURITY

This Strategy articulates the overall aim and objectives of the Australian Government's cyber security policy and sets out the strategic priorities that the Australian Government will pursue to achieve these objectives. The Strategy also describes the key actions and measures that will be undertaken through a comprehensive body of work across the Australian Government to achieve these strategic priorities.

In developing this Strategy the Australian Government undertook a comprehensive review of Australia's cyber security policies, capabilities and arrangements in 2008.

This Strategy will guide the efforts of Australian Government agencies towards the achievement of the Australian Government's policy objectives. This includes the work of Australia's intelligence, security, law enforcement and regulatory agencies. Importantly, the Strategy also provides a clear public articulation of the Australian Government's approach to cyber security. This is in recognition that, while the Australian Government has an important leadership role, effective cyber security efforts can only be achieved through partnerships between government, business and the community, in Australia and internationally.

## Aim

The aim of the Australian Government's cyber security policy is:

> ***The maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy.***

## Scope

The Australian Government defines cyber security as:

> ***Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.***

The Australian Government recognises that, from the perspective of an Australian Internet user, protecting yourself online is not simply a matter of securing your computer. It is also about sensible online practices, such as protecting your identity and privacy and understanding how to respond to fraudulent emails, cyber-bullying or stalking. This includes parents who are concerned about their children's activities online, where as a result of their actions they may expose the computer to a virus or expose themselves to offensive content, cyber-bullying or individuals seeking to groom them for the purposes of sexual exploitation.

This Strategy does not seek to address all of these risks. It is focused on the availability, integrity and confidentiality of Australia's ICT. However, it is essential that it works in harmony with other related policies and programs, including cyber safety, identity security and privacy.

In particular, the Australian Government's cyber security policy must be coordinated with its approach to cyber *safety*, which is focused on protecting individuals, especially children, from exposure to illegal and offensive content, cyber-bullying, and grooming online for the purposes of sexual exploitation.

In addition, there is a strong linkage between this Strategy and the Commonwealth Organised Crime Strategic Framework and the efforts of all governments to respond to the threats posed by organised crime. In particular, this Strategy will be a contributing element to the development of the Organised Crime Response Plan and specific cyber security capabilities and arrangements will be of value for outreach to the community and the private sector on organised crime and in deepening the understanding of the use of new technologies to enable the commission of organised crime.

### Cyber Safety Plan

Cyber safety concentrates on the broader social and personal risks associated with the use of technology, particularly in relation to children. These include issues such as cyber-bullying, sexual grooming, exposure to illegal and inappropriate content, loss of personal information and the promotion of inappropriate social and health behaviours.

In May 2008, the Australian Government committed $125.8 million over four years to a comprehensive range of cyber safety measures.

The Cyber Safety Plan's measures include:

- the expansion of the Australian Federal Police (AFP) Child Protection Operations Team to detect and investigate online child sex exploitation
- the Commonwealth Director of Public Prosecutions helping deal with increased activity resulting from the work of the AFP to ensure that prosecutions are handled quickly
- the examination of the introduction of Internet service provider (ISP) level filtering of Refused Classification material under the existing National Classification Code and whether additional ISP content filtering options should be available for those families who wish to have such a service
- education and outreach activities through the Australian Communications and Media Authority (ACMA) to implement a comprehensive range of education activities
- a Consultative Working Group to consider the broad range of cyber safety issues and provide advice to the Australian Government to ensure properly developed and targeted policy initiatives
- a Youth Advisory Group and online forum to provide advice on cyber safety issues from a young person's perspective, and
- research into the changing digital environment to identify issues and target future policy and funding.

More information on the Cyber Safety Plan is available at www.dbcde.gov.au

## National Identity Security Strategy

The National Identity Security Strategy aims to maximise the effectiveness and interoperability of work across all levels of government to combat the misuse of stolen or assumed identities.

The preservation and protection of a person's identity is a right of all Australians. Identity theft is a major invasion of privacy and a serious concern to the community. To combat identity crime and to better protect identities, Australian governments have all agreed to the development and implementation of the National Identity Security Strategy. The Strategy enhances identification processes through:

- improved registration and enrolment procedures, including a new system for the electronic verification of documents used as evidence of identity
- enhanced security features on identity documents issued by government agencies, reducing the risk of forgery
- ensuring accuracy in the identity information held by government agencies
- strong authentication standards, and
- biometric interoperability, to confirm the identity of individuals.

Australian governments, in collaboration with the private sector, are working to enhance identity security for all, particularly as business is increasingly conducted online.

More information on the National Identity Security Strategy, including advice to individuals on how to help protect themselves from identity theft and what to do if identity information has been stolen or fraudulently used, is available at www.ag.gov.au

## Guiding principles

Consistent with the enduring principles outlined in the National Security Statement, the Australian Government's cyber security policy is based on the following guiding principles:

***National leadership:*** The scale and complexity of the cyber security challenge requires strong national leadership. The Australian Government regulates the communications infrastructure on which both private and public ICT depends. The national and transnational nature of these technologies makes the Australian Government best placed to identify the strategic threats and emerging challenges to Australia's cyber security. Furthermore, as a trustee of the private and personal information of Australians, the Australian Government can model and influence best practice in cyber security.

***Shared responsibilities:*** All users, in enjoying the benefits of ICT, should take reasonable steps to secure their own systems, exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users.

***Partnerships:*** In light of these shared responsibilities, a partnership approach to cyber security across all Australian governments, the private sector and the broader Australian community is essential.

***Active international engagement:*** Given the transnational nature of the Internet, in which effective cyber security requires coordinated global action, Australia must adopt an active, multi-layered approach to international engagement on cyber security. This includes engagement with other countries who share the Australian Government's concerns about cyber security and through organisations examining these issues, including the United Nations, International Telecommunication Union (ITU), Asia Pacific Economic Cooperation (APEC) and the Organisation for Economic Cooperation and Development (OECD).

***Risk management:*** In a globalised world where all Internet-connected systems are potentially vulnerable and where cyber attacks may be difficult to detect, there is no such thing as absolute cyber security. Therefore, when Australia is assessing, prioritising and resourcing cyber security activities it should consider where the greatest areas of risk to the national interest lie.

***Protecting Australian values:*** Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms. Maintaining this balance is a continuing challenge for all modern democracies seeking to meet the complex cyber security challenges of the future.

## Roles and responsibilities of Australian Government agencies

The Attorney-General's Department is the lead agency for cyber security policy across the Australian Government and chairs the Cyber Security Policy and Coordination (CSPC) Committee, which is the interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.

Integral to the Australian Government's Cyber Security Strategy are two key organisations: CERT Australia and the Cyber Security Operations Centre (CSOC). A range of agencies contribute to the implementation of the Strategy and the operation of CERT Australia and the CSOC. A detailed description of the role of Australian Government agencies is at Attachment A.

## CERT Australia

The Australian Government is bringing together Australia's national computer emergency response team (CERT) arrangements into a new Government operated national CERT, CERT Australia. This will enable a more integrated, holistic approach to cyber security across the Australian community by creating a single coordination point within the Australian Government for the provision of information and advice.

CERT Australia will incorporate a range of current cyber security activities undertaken by existing Australian Government agencies, including the Australian Government's Computer Emergency Readiness Team (GovCERT.au) in order to:

- provide Australians with access to information on cyber threats, vulnerabilities in their systems and information on how to better protect themselves
- promote greater shared understanding between government and business of the nature and scale of cyber threats and vulnerabilities within Australia's private sector networks and how these can be mitigated
- provide targeted advice and assistance to enable the owners and operators of critical infrastructure and other systems of national interest to defend their systems from sophisticated electronic attacks, working in close collaboration with intelligence and law enforcement agencies, via the newly established Cyber Security Operations Centre (CSOC), and
- provide a single Australian point of contact in the expanding global community of national CERTs to support more effective international cooperation.

CERT Australia will commence operations as the national CERT in early 2010.

More information on CERT Australia can be found at www.cert.gov.au

## Cyber Security Operations Centre

Established as an initiative of the Australian Government's Defence White Paper, the Cyber Security Operations Centre (CSOC) provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance.

The CSOC's core functions include:

- providing comprehensive understanding of the cyber threat and the security status of government networks and networks of national importance
- identifying and analysing sophisticated cyber attacks and providing government with response options, and
- assisting responses to cyber events across:
  - government, and
  - critical private sector systems and infrastructure through the Joint Operating Arrangements and the Attorney-General's Department.

More information on the CSOC can be found at www.dsd.gov.au

# OBJECTIVES

The Australian Government's cyber security policy is based on three key objectives.

**OBJECTIVE ONE: ALL AUSTRALIANS ARE AWARE OF CYBER RISKS, SECURE THEIR COMPUTERS AND TAKE STEPS TO PROTECT THEIR IDENTITIES, PRIVACY AND FINANCES ONLINE**

The Australian Government recognises the importance of building and maintaining the confidence of all Australians to participate in the digital economy. The Australian Government is committed to informing and educating Australians on cyber security risks and empowering them with the knowledge and practical tools to protect themselves online.

As the Internet continues to be integrated into more aspects of daily life and more and more personal and financial information is being placed online, cyber crime is becoming an increasing concern to many Australians. There is potential for this to be further exacerbated by the growth in 'always on' broadband connections and the increased bandwidth associated with next generation networks.

The inherent characteristics of a borderless, lightly regulated and largely anonymous online environment make it impossible to prevent all security incidents from occurring. However, government and business must strive to limit cyber security risks to the Australian community from becoming so chronic or widespread as to undermine confidence in the digital economy. There is a reasonable expectation that governments and the private sector, including the Internet industry, will educate users and their customers on the risks and the steps they can take to minimise them.

A key role for the Australian Government is, therefore, to promote a robust culture of cyber security that provides all Australians with the awareness and confidence to maximise the benefits that the digital economy has to offer, while minimising their exposure to the risks of the online environment.

In this environment, all Australians need to take reasonable steps to ensure the protection of their personal information and Internet-connected ICT systems. In order to do this effectively, users need to be aware of the risks of being online and the relatively straightforward steps that they can take to protect their systems and their information online.

The importance of this objective goes well beyond the protection of individuals, as compromised home computers can readily be organised into 'botnets' that may be used to launch attacks against government or other critical systems.

By empowering all users with the knowledge and confidence to protect their information and systems online, the Australian Government can help reduce the impact of cyber crime and mitigate the threat to systems critical to the national interest. Moreover, by addressing some of the systemic vulnerabilities in Australian networks, the Australian Government can strengthen Australia's ability to advocate similar 'best practice' approaches to cyber security in the international arena in order to support efforts to promote a more secure and resilient online environment.

## OBJECTIVE TWO: AUSTRALIAN BUSINESSES OPERATE SECURE AND RESILIENT INFORMATION AND COMMUNICATIONS TECHNOLOGIES TO PROTECT THE INTEGRITY OF THEIR OWN OPERATIONS AND THE IDENTITY AND PRIVACY OF THEIR CUSTOMERS

Business and government have shared interests and responsibilities for ensuring a secure and reliable electronic operating environment on which both business and government services depend.

As the Australian Government does not own the majority of the systems that are critical to the community, it needs to identify ways in which it can influence the policies and practices of those that do. This includes State and Territory government systems, government-business enterprises, and organisations and companies operating in the private and non-government sectors. These systems are critical to Australia's national interest and are therefore in need of particular and specific attention, including direct support from the Australian Government.

For these reasons, the Australian Government works with the private sector to identify the systems that are most critical to Australia's national interest, based on an assessment of risk that considers factors such as: uniqueness, importance, vulnerability and attractiveness to potential adversaries.

The Australian Government maintains trusted relationships with the owners and operators of systems that are considered to be most critical to Australia's national interests. Working through trusted information exchange mechanisms, the Australian Government provides these organisations with a better understanding of the cyber threat environment to build a greater shared understanding of threats and vulnerabilities. By gaining a greater awareness and understanding of these largely privately owned systems of national interest, the Australian Government can better tailor its assistance to the owners and operators of systems of national interest. This may extend to providing targeted advice and assistance in responding to sophisticated electronic threats.

An understanding of the impact that a disruption to these systems would have on the national interest is an essential part of the Australian Government's ability to manage a crisis. Cyber events need to be managed in a coordinated and timely manner. The Australian Government will put in place a plan to ensure the continuity of government and critical services when a cyber event occurs.

The Australian Government is also committed to working with the broader business community to optimise cyber security across the whole of the digital economy, by promoting a greater awareness of cyber security risks and best practice approaches to how these can be mitigated. With this knowledge and these tools Australian businesses can be empowered to ensure the security of their own ICT systems and protect valuable customer information.

Australian businesses are increasingly being entrusted with large amounts of financial and other personal information on behalf of their customers. The aggregation of this data can present an attractive target for cyber criminals and businesses should therefore be mindful of their responsibilities for protecting this information. These responsibilities also extend to providing secure, trusted environments in which their customers can transact online.

Business is responsible for the security and reliability of their systems and infrastructure and the transactions that take place on them. Maintaining consumer confidence in transacting online is fundamental to the success of the digital economy.

**What are systems of national interest?**

In today's modern digital economy, systems of national interest go beyond traditional notions of critical infrastructure such as electricity grids, water storage and distribution, aviation and maritime transport, and telecommunications networks. They also include, for example, systems of high economic value such as those that support electronic transactions, hold sensitive intellectual property such as biotechnology patents or other commercial data associated with major international trade negotiations.

They are the systems which, if rendered unavailable or otherwise compromised, could result in significant impacts on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security.

The identification of systems of national interest is not a static process and a flexible approach is required to enable the Australian Government to respond to the changing environment–in terms of technology, usage, threat and risk. It is for this reason that the identification of systems of national interest must be informed by an ongoing assessment of risk.

## Control systems security

Control systems, which include supervisory control and data acquisition (SCADA) systems, are devices and networks used to electronically control mechanical processes such as water valves, electricity generation and transmission or the operation of a coal loader. Using these systems, operators are able to monitor processes and control infrastructure, from across the road or across the globe. Control systems are increasingly being interconnected with corporate business networks and, directly or indirectly, to the Internet. This, together with rapid advances in technology, changing business needs, and the increasing threat environment associated with the Internet, is compounding the vulnerability of control systems to cyber threats.

The Australian Government is working with control systems owners and operators to help them secure their systems. Under the auspices of the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), the Australian Government has:

- provided guidance and advice to TISN member organisations on control systems security in the form of advisories and alerts on specific vulnerabilities and threats to control systems and networks
- established a SCADA Community of Interest to provide a forum to raise the awareness of security for control systems practitioners from critical infrastructure sectors, vendors, consultants and researchers, and
- supported control systems practitioners participating in world's best practice training in advanced control systems cyber security conducted in the United States.

The Australian Government, through CERT Australia, operates trusted information exchanges with the owners and operators of control systems. This enables government and business to share sensitive and detailed technical security information, thereby building a greater understanding of the control systems environment and its threats.

CERT Australia is also partnering with Australian academic organisations, such as Edith Cowan University, on vulnerability and mitigation research programs looking at initiatives such as smartgrids and smart metering technologies and their security implications.

## OBJECTIVE THREE: THE AUSTRALIAN GOVERNMENT ENSURES ITS INFORMATION AND COMMUNICATIONS TECHNOLOGIES ARE SECURE AND RESILIENT

The ICT systems of government and the information contained within them are a strategic national asset. The Australian Government therefore has a clear responsibility for ensuring the security and resilience of its own ICT, including protecting the information it holds about Australian people and organisations.

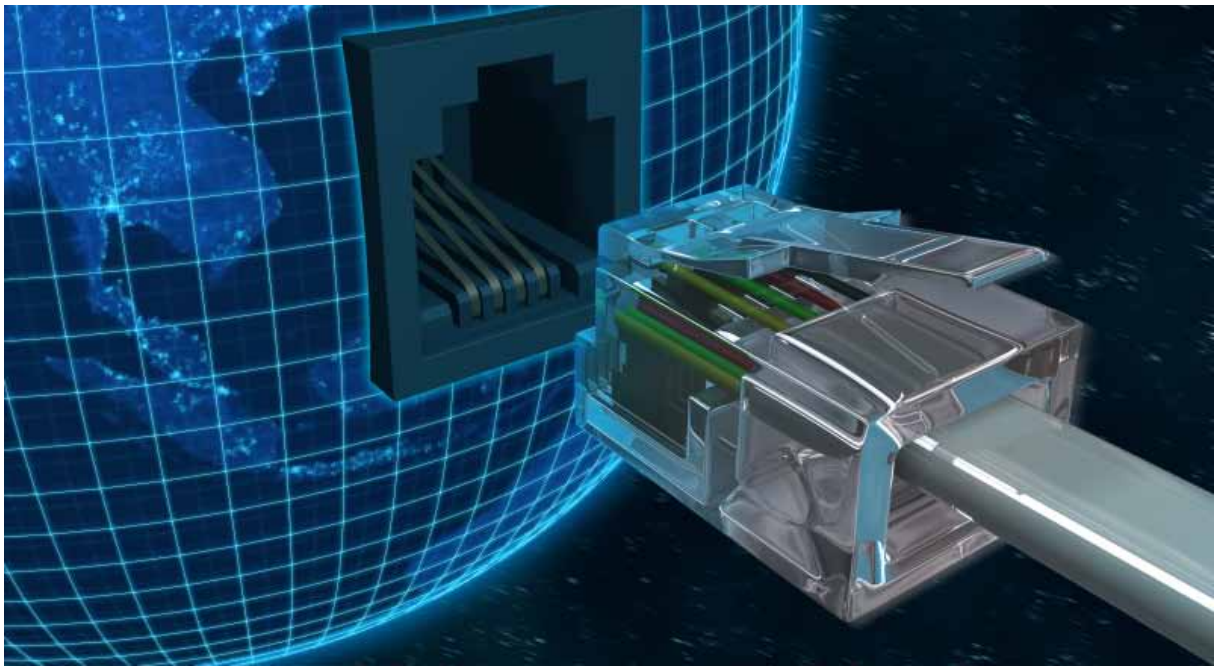
The Australian Government can only protect its information and ICT from threats and vulnerabilities that it has identified. It is critical that the Australian Government is proactive in identifying and understanding these threats and vulnerabilities to ensure the development of appropriate mitigation strategies.

In order to achieve this objective, the Australian Government will enhance its understanding of the cyber threat environment and respond appropriately to protect Australian Government information and ICT.

Additionally, the Australian Government needs to have in place a consistent and integrated framework of policies, procedures and technical standards to ensure the protection of its information and ICT – one that recognises the security of systems as a fundamental component of all Australian Government initiatives dependent upon ICT.

This framework needs to be applied not only to Australian Government systems, but also the interconnected government systems, such as e-health, that are increasingly being developed to assist in shared service delivery between the Commonwealth and the States and Territories.

However, government systems represent only a fraction of the global ICT infrastructure on which Australia's economic and national security depends. The Australian Government is committed to leading by example by embracing best practice in the protection of the Australian Government's own information systems, including the protection of the personal and corporate information entrusted to it. By specifying minimum security standards that apply across government, the Australian Government can create incentives for the market to make more secure services available to the public.



# STRATEGIC PRIORITIES

In order to achieve these objectives, the Australian Government is undertaking a comprehensive body of work based around the following set of integrated, mutually supporting strategic priorities.

There are clear linkages between many of these priorities and the broader objectives of the Strategy, for example, in relation to government systems. However, it is important to note that the priorities support the achievement of all objectives. For example, international engagement, including the sharing of information and expertise and the development of collaborative approaches, serves as an enabler to all cyber security activities.

**PRIORITY: THREAT AWARENESS AND RESPONSE – IMPROVE THE DETECTION, ANALYSIS, MITIGATION AND RESPONSE TO SOPHISTICATED CYBER THREATS, WITH A FOCUS ON GOVERNMENT, CRITICAL INFRASTRUCTURE AND OTHER SYSTEMS OF NATIONAL INTEREST**

This priority covers initiatives to maintain capabilities for continuous, real-time monitoring of the online threat environment, supported by established plans for responding to events should they occur.

Under this priority the Australian Government is undertaking a range of measures including:

- establishing a Cyber Security Operations Centre (CSOC) within the Department of Defence to provide a 24/7 cyber situational awareness capability and coordinate responses to cyber security events of national importance
- creating a new national computer emergency response team, CERT Australia, to share information and improve the coordination of responses to cyber security threats between government and the private sector
- actively participating in and facilitating trusted and timely information sharing within and between government and business, nationally and internationally, to ensure the maintenance of situational awareness and a consistent, global response to online threats
- developing an updated cyber security crisis management plan that outlines the arrangements for responding to cyber security events of national significance, including coordination with the States and Territories and the private sector, and
- conducting a program of cyber security exercises to test and refine event response arrangements, including the Cyber Storm series of exercises coordinated by the United States.

### Cyber Storm

The United States Department of Homeland Security sponsors a series of large scale cyber security exercises collectively called Cyber Storm. Cyber Storm gives participants the opportunity to exercise their internal event response and communications in a national framework that is part of an international exercise.

In March 2008, 56 Australian organisations from across government and the private sector participated in the second large-scale international cyber exercise, Cyber Storm II, along with a broad range of government and non-government organisations from the United States, Canada, New Zealand and the United Kingdom. This exercise provided an opportunity for stakeholders across the spectrum of cyber security and critical infrastructure in Australia to test their disaster recovery, communications and technical response processes to a cyber security event.

Australia will participate in Cyber Storm III to be held in late September 2010.

## PRIORITY: CULTURAL CHANGE – EDUCATE AND EMPOWER ALL AUSTRALIANS WITH THE INFORMATION, CONFIDENCE AND PRACTICAL TOOLS TO PROTECT THEMSELVES ONLINE

Australians use ICT for a wide variety of purposes and at an ever-increasing rate. In order to ensure their personal and financial information and their identity and privacy are protected, it is essential that they maintain an awareness and understanding of the cyber environment and its risks.

This priority covers initiatives to conduct education and awareness raising activities to promote a culture of cyber security amongst all Australian ICT users.

Under this priority the Australian Government is undertaking a range of measures including:

- a single authoritative website for cyber security information for Australian home users and small business including those with limited cyber security knowledge and skills (www.staysmartonline.gov.au).

  This website includes plain language alerts and advisories for the public including information on new cyber security risks and how to address them
- the creation of CERT Australia to ensure the Australian Internet community has access to information on cyber security threats, vulnerabilities in their systems and information on how to better protect their information technology environment
- practical tools, such as the SpamMATTERS[5] reporting tool to address the growing problems of spam
- broader engagement with the commercial Internet industry, including working with industry on the development of a voluntary Internet service provider (ISP) Code of Practice to promote best practice approaches to deal with cyber security issues
- cyber security education modules for Australian primary and secondary schools
- an ongoing program of awareness raising, culminating in an annual Cyber Security Awareness Week, conducted in partnership with business, consumer groups and community organisations, and
- examining options to better inform and educate the community on a broad range of online risks, including cyber security, identity security, cyber safety and online fraud.

[5] Further information on SpamMATTERS is available at www.acma.gov.au

### Australian Internet Security Initiative

The Australian Internet Security Initiative (AISI) helps address the problem of compromised computers (sometimes referred to as 'zombies' or 'bots'). Computers can become compromised through the installation of malicious software (malware) without a user's knowledge or consent that enables the computer to be controlled remotely for illegal and harmful activities.

Compromised computers are often combined into large groups known as 'botnets'. Among other things, 'botnets' are used for the mass distribution of spam and spyware, the hosting of 'phishing' sites designed to steal users' personal information and distributed denial of service attacks on websites to render them inaccessible.

On average, there were 4,291 AISI compromise reports per day over the 2008-09 year. On an annual basis, this represents 1.57 million discrete AISI reports.

The AISI collects data from various sources on computers exhibiting 'bot' behaviour on the Australian Internet. Using this data, the Australian Communications and Media Authority (ACMA) provides daily reports to participating Internet service providers (ISPs) identifying computers on their networks that have been reported to have been compromised in the previous 24-hour period. ISPs can then inform their customer that their computer appears to be compromised and provide advice on how they can fix it.

There are 71 ISPs that participate in the program (as at October 2009). ACMA intends to progressively increase the number of ISPs participating in the AISI to ensure that more compromised hosts on the Australian Internet are identified and their owners notified of the compromise.

More information on the AISI can be found at www.acma.gov.au

## PRIORITY: BUSINESS-GOVERNMENT PARTNERSHIPS – PARTNER WITH BUSINESS TO PROMOTE SECURITY AND RESILIENCE IN INFRASTRUCTURE, NETWORKS, PRODUCTS AND SERVICES

The Australian Government recognises that the economic and social wellbeing, national security and defence of Australia is often dependent upon systems that are owned and operated outside the Australian Government.

This priority therefore recognises that government and business must work together to provide more secure products and services and maintain their ICT systems in ways that ensure the privacy and security of customer information. It recognises that ISPs, in particular, occupy a unique position at the gateway to Australians' access to the Internet and therefore need to be a key partner in the Australian Government's efforts to maximise the cyber security of all Australians.

It also recognises that vulnerabilities in Australia's critical infrastructure and other systems of national interest represent a greater level of risk to Australia's national security than systems supporting broader online commerce and that a more intensive level of engagement is required between government and the owners and operators of these systems of national interest. It covers initiatives

that enable the Australian Government to develop greater situational awareness of potential vulnerabilities in critical private sector networks, while also providing mechanisms for the Australian Government to provide tailored information and targeted assistance to the owners and operators of these networks for dealing with sophisticated cyber threats.

Under this priority the Australian Government is undertaking a range of measures including:

- using CERT Australia to strengthen trusted partnerships with the private sector for the sharing of sensitive information on cyber threats, vulnerabilities and their potential consequences.

  This includes tailored alerts and advisories for Australian businesses and more intensive trusted information exchanges with high risk sectors to share information on sophisticated threats. These exchanges cover the telecommunications and banking and finance industries and the owners and operators of the control systems that underpin much of the nation's critical infrastructure
- strengthening engagement with the commercial Internet industry to raise awareness of cyber security risks, identify cyber threats and vulnerabilities and appropriate mitigation strategies, including through:
  - ISP participation in the Australian Internet Security Initiative, and
  - working with industry on the development of a voluntary ISP Code of Practice to promote best practice approaches to deal with cyber security issues
- broader engagement with business via the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) to promote integrated, best practice approaches to cyber security and critical infrastructure protection based on the concept of resilience
- providing world-leading computer modelling capabilities for business and government via the Critical Infrastructure Protection Modelling and Analysis (CIPMA) program, which models the complex relationships between critical infrastructure systems and shows how a failure in one sector can greatly affect the operations of other sectors
- facilitating access for industry representatives, including those working with critical systems in the area of control systems, to education and training opportunities through collaboration with foreign governments and educational institutions
- working with Standards Australia and other industry bodies to develop and promote best practice standards, and
- ensuring that security issues are addressed in the design and operation of the NBN.

### Critical Infrastructure Protection & the Trusted Information Sharing Network for Critical Infrastructure Protection

Since the creation of the Critical Infrastructure Protection (CIP) Program in 2003, its primary focus has been to share information and best practice with the owners and operators of critical infrastructure, to strengthen and improve their security measures and to help inform their risk management.

*Critical infrastructure* is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security.

The CIP Program is transitioning to a focus on building organisation *resilience*. Organisation resilience takes a holistic approach that seeks to break down the silos of security, risk, emergency and business continuity management to help an organisation adapt, survive and possibly thrive in a crisis.

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is a forum where the owners and operators of critical infrastructure work together, sharing information on the security issues that affect them. It provides a trusted environment where industry and government can share vital information on critical infrastructure protection and organisational resilience. The TISN has established a truly collaborative relationship between business and government based on trust that is helping to build a more resilient Australia.

The TISN comprises nine Infrastructure Assurance Advisory Groups (IAAGs), each representing different critical infrastructure sectors as follows: banking and finance, communications, emergency services, energy, food chain, health (private), water services, mass gatherings, and transport (aviation, maritime and surface). The role of the IAAGs is to allow critical infrastructure owners and operators to work together and share information on threats and vulnerabilities and appropriate measures and strategies to mitigate risk. The participation of government agencies, both Commonwealth and State and Territory, in the IAAGs assist in building a greater shared understanding of CIP issues.

Of particular relevance to cyber security is the TISN's Communications Sector IAAG which brings together telecommunications, international submarine cables, postal and broadcasting owners and operators with the aim of enhancing the resilience of the sector to all hazards, including cyber.

More information on the TISN can be found at www.tisn.gov.au

**PRIORITY: GOVERNMENT SYSTEMS – MODEL BEST PRACTICE IN THE PROTECTION OF GOVERNMENT ICT SYSTEMS, INCLUDING THE SYSTEMS OF THOSE TRANSACTING WITH GOVERNMENT ONLINE**

This priority recognises that the ICT systems of government, and the information contained within them, is a strategic national asset. It covers initiatives to protect Australian Government systems and interconnected government systems that are increasingly being developed to assist in shared service delivery between the Commonwealth and the States and Territories. It also includes reforms to whole of government ICT procurement arrangements that provide cost efficiencies and specify minimum security standards that apply across government. These reforms have the potential to create incentives for the market to make more secure services available to the public.

Under this priority the Australian Government is undertaking a range of measures including:

- examining options to reduce the number of Australian Government Internet gateways to the minimum number practical so as to maximise efficiency, reliability and security
- establishing more effective minimum security standards across government, including through reforms to achieve a more centralised approach to the procurement and management of ICT products and services. This includes requiring cyber security risk assessments for all major Australian Government ICT projects
- partnering with State and Territory governments and other key stakeholders to promote the effective security of interconnected government systems, including through consideration of relevant Australian Government security standards, and
- reviewing the Australian Government's Protective Security Manual to ensure that its information security policies and standards continue to keep pace with developments in technology and reflect international best practice. The aim of this review will be to, wherever practicable, link Australian Government requirements to corresponding commercial standards to promote the adoption of similar best practice approaches across the private sector.

### OnSecure

OnSecure is a cooperative project between the Defence Signals Directorate (DSD) and the Australian Government Information Management Office. It aims to improve the collection of information security event reports in the Australian Government and improve the analysis of such events. Information on potential threats, vulnerabilities and mitigation from this analysis is then disseminated via OnSecure for all government agencies. OnSecure is the central Australian Government Internet site for information security material provided by DSD.

**PRIORITY: INTERNATIONAL ENGAGEMENT – PROMOTE A SECURE, RESILIENT AND TRUSTED GLOBAL ELECTRONIC OPERATING ENVIRONMENT THAT SUPPORTS AUSTRALIA'S NATIONAL INTERESTS**

As an open, democratic society that is fully enmeshed in the globalised economy, Australia's economic prosperity and national security is now fundamentally reliant on a secure and resilient online environment.

The global challenge of cyber security requires an increased effort in multilateral forums to improve the security of interoperable networks. This includes the United Nations and the ITU, regional forums such as APEC and more subject specific international groups such as the Forum of Incident Response and Security Teams (FIRST) and the International Watch and Warning Network (IWWN). International efforts include the development of global standards, expansion of the international legal system's capacity to combat cyber crime and the development and promotion of best practice in situational awareness, strategic warning and event response.

Under this priority the Australian Government is pursuing an active approach to international engagement on cyber security through:

- bilateral or multilateral agreements with key allies and other likeminded nations to strengthen cooperation on cyber security
- regional forums, with a focus on capacity building initiatives within our region
- international organisations to help promote international best practice and develop and foster a coordinated global approach to combating cyber security threats, including spam, and
- developing an international engagement strategy to clearly define and articulate Australia's national interests and priorities in relation to cyber security and resilience.

  This strategy will identify priority areas for Australia's engagement in each of the above areas to help ensure that Australia's diplomatic, security, law enforcement and broader government efforts are coordinated and targeted towards the achievement of Australia's national interests.

**PRIORITY: LEGAL AND LAW ENFORCEMENT – MAINTAIN AN EFFECTIVE LEGAL FRAMEWORK AND ENFORCEMENT CAPABILITIES TO TARGET AND PROSECUTE CYBER CRIME**

This priority recognises the increasing impact of cyber crime on the Australian economy and society. This includes organised crime which is increasingly making use of technology to fund, enable the commission of and avoid law enforcement and regulatory detection and disruption of crime. It covers initiatives to maintain a strong legal framework, associated investigative and enforcement capabilities and a technically-aware legal system to combat this growing challenge, both domestically and internationally.

**What is cyber crime?**

**The Australian Government defines cyber crime as those computer offences under** the *Commonwealth Criminal Code Act 1995* **(Part 10.7) which involve the unauthorised access to, modification or impairment of electronic communications.**

Under this priority the Australian Government is undertaking a range of measures including:

- providing additional resources for security and law enforcement agencies to enhance operational capabilities for combating cyber crime and other cyber security threats
- ensuring that linkages are in place between cyber security and law enforcement efforts to combat specific related crime types, including organised crime, through the sharing of information and intelligence
- in partnership with State and Territory governments, ensuring Australia's criminal and civil legal framework is robust and keeps pace with developments in technology and criminal behaviour. For example, the Australian Government has introduced new legislation to provide a firmer legal basis for legitimate computer network protection activities through amendments to the *Telecommunications (Interception and Access) Act 1979*
- providing Australian legal professionals with access to information and resources to provide them with the requisite level of technological knowledge and understanding to effectively administer these laws, and
- promoting the harmonisation of Australia's legal framework for cyber security with other jurisdictions and internationally to facilitate information sharing and law enforcement cooperation across geographical borders.

### Legal Framework

Australia has a comprehensive cyber security legal framework, comprising Commonwealth and State and Territory legislation. At the Commonwealth level, the key elements of this framework include:

- *Criminal Code Act 1995 (*as amended by the *Cybercrime Act 2001)*
- *Telecommunications (Interception and Access) Act 1979*
- *Spam Act 2003*
- *Telecommunications Act 1997,* and
- *Privacy Act 1998.*

Other relevant Commonwealth legislation includes:

- *Surveillance Devices Act 2004*
- *Intelligence Services Act 2001,* and
- *Australian Security Intelligence Organisation Act 1979*.

### Organised Crime Strategic Framework

Organised crime costs Australia in the order of $10 to $15 billion each year. These costs impact on all Australian governments and businesses. Organised crime also causes great harm to individuals and the broader community. Organised criminal networks are flexible, innovative and resilient. These networks are profit driven, constantly looking for new opportunities and operating across state, territory and national borders. To respond to these challenges the Australian Government has developed the Commonwealth Organised Crime Strategic Framework. The Framework establishes a comprehensive and coordinated response to target the most significant threats from organised crime in order to reduce its impact on the community. The Framework will ensure our law enforcement, intelligence, policy and regulatory agencies are collaborating effectively with each other, with their State and Territory counterparts and with Australian businesses and the community to combat organised crime.

**PRIORITY: KNOWLEDGE, SKILLS AND INNOVATION – PROMOTE THE DEVELOPMENT OF A SKILLED CYBER SECURITY WORKFORCE WITH ACCESS TO RESEARCH AND DEVELOPMENT TO DEVELOP INNOVATIVE SOLUTIONS**

A technically skilled workforce, supported by cutting edge research and development, is fundamental to Australia's ability to develop innovative solutions to emerging cyber security challenges. This priority covers initiatives to build and retain this expertise within government and to harness the resources of Australia's research community in support of the Australian Government's cyber security efforts.

Under this priority the Australian Government is undertaking a range of measures including:

- developing recruitment and retention strategies aimed at ensuring a sufficient level of technical expertise is developed and maintained within government agencies
- providing targeted funding and support for cyber security research and development activities through a range of programs such as the Research Support for National Security Program.

  This includes not only technological areas such as quantum cryptography, but may also include research into areas of behavioural change, policy and market-based incentive mechanisms to address systemic cyber security issues, and
- developing an annual set of research and development priorities to inform the broader science and innovation community of the priority work required to achieve the Australian Government's cyber security policy.

  This work is being taken forward via the Australian Government's National Security Science and Innovation Strategy, which identifies cyber security as one of 12 priority areas where science and innovation can enhance Australia's national security.

### National Security Science and Innovation Strategy

The National Security Science and Innovation Strategy (NSSIS) aims to enhance the application of science and innovation to national security. The NSSIS encourages better targeted resource allocation through clearly defined national security objectives and priorities for science and innovation. The NSSIS policy framework aligns the national security and science and innovation policy environments by providing a balanced approach to delivering national security science and innovation outcomes that meet immediate requirements while building the capacity to meet longer term challenges.

### Critical Infrastructure Protection Modelling and Analysis

One example of how science and innovation supports the Australian Government's Cyber Security Strategy is the Critical Infrastructure Protection Modelling and Analysis (CIPMA) program. CIPMA is a world-leading computer modelling program that acts as a key component of the Australian Government's efforts to enhance critical infrastructure protection. Based on a strong business-government partnership, CIPMA models and examines the complex relationships and interdependencies between critical infrastructure systems, and shows how a failure in one sector can greatly affect the operations of other sectors.

CIPMA enjoys strong support from the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), with five sectors (banking and finance, communications, energy, water services and transport) currently engaged in the program.

# CONCLUSION

Due to the pace of technological change and broader developments in the online threat environment, it is necessary to undertake ongoing evaluation and regular reviews of the appropriateness of Australian Government cyber security activities.

The process of evaluating the effectiveness of the cyber security policy will be undertaken as part of the broader national security strategic evaluation framework announced in the Prime Minister's National Security Statement.

The Australian Government will regularly review Australia's cyber security policies, programs and capabilities. This will ensure that the efforts of the Australian Government remains focussed on maintaining a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy. This will be done in close collaboration with the States and Territories, the private sector and the broader community.

# ATTACHMENT A – AUSTRALIAN GOVERNMENT GOVERNANCE ARRANGEMENTS

At the forefront of the Australian Government's Cyber Security Strategy are two key organisations, currently being established and expected to be fully operational in early 2010:


## CERT Australia – Australia's national computer emergency response team

The Attorney-General's Department will progressively take responsibility for the national computer emergency response team (CERT) function for Australia – CERT Australia will commence operations in early 2010.

CERT Australia will bring together Australia's existing computer emergency response arrangements under a new national CERT. It will provide a single point of contact for cyber security information for all Australians and Australian businesses and ensure Australian Internet users have access to information on cyber threats, vulnerabilities in their systems and information on how to better protect their information technology environment.

It will incorporate a range of current cyber security activities undertaken by Australian Government agencies, including the Australian Government Computer Emergency Readiness Team (GovCERT.au).

CERT Australia will complement the work of the Cyber Security Operations Centre (CSOC).


## Cyber Security Operations Centre (CSOC)

The CSOC in the Defence Signals Directorate is a Defence capability serving whole of government cyber security needs to detect and defeat sophisticated cyber threats. The CSOC provides cyber situational awareness and an enhanced ability to facilitate coordinated responses to, and management of, cyber security events of national importance. Staffed by skilled experts from a number of Australian

Government agencies, it maximises the Australian Government's ability to prevent, detect and rapidly respond to fast evolving sophisticated cyber exploitation attempts and attacks.

The CSOC draws on an array of sources in the intelligence and security, law enforcement, national CERT and industry communities to provide a comprehensive picture of threats to Australian information and systems. The CSOC coordinates cyber event responses by government agencies and works in collaboration with overseas partners. It will accommodate a continuously staffed watch office and analysis team able to prevent or respond immediately to significant cyber threats as they are detected.

## Australian Government agencies

A range of agencies make a significant contribution to the implementation of the Australian Government Cyber Security Strategy and the operation of CERT Australia and the CSOC. Recognising that all Australian Government agencies have an important role to play in ensuring the security and resilience of Australian Government systems, the following agencies have clear responsibility for the delivery of Australian Government cyber security outcomes.

The **Attorney-General's Department** (AGD) is responsible for Australian Government protective security policy and for criminal law and law enforcement policy, including:

- providing whole of government coordination on cyber security policy, including crisis management and international collaboration
- promulgating protective security policy for Australian Government agencies
- taking a leadership role in advancing business-government partnerships, including national CERT arrangements, and
- providing cyber security guidance to owners and operators of critical infrastructure and other businesses of national interest.

CERT Australia works with the Joint Operating Arrangements (JOA) agencies to contribute to a shared understanding of major events, provide a pathway to the national crisis management arrangements, and be able to provide alerts and guidance to the private sector.

The **Australian Communications and Media Authority** (ACMA) is responsible for the regulation of broadcasting, the Internet, radiocommunications and telecommunications. It contributes to cyber security objectives by:

- gathering evidence and assisting in protecting Australians from computer fraud and identity theft
- ensuring Internet service providers (ISPs) and telecommunications providers are meeting their regulatory obligations regarding criminal misuse and illegal content
- encouraging the development of codes of practice for ISPs and online content service providers and monitoring compliance with these codes
- working with ISPs for the identification of compromised computers, and
- identifying, investigating and acting against those involved in the distribution of spam.

The **Australian Federal Police** (AFP) enforces Commonwealth criminal law and protects Commonwealth and national interests from crime in Australia and overseas. In relation to cyber security, the AFP:

- provides a specialised investigative capacity to support the identification, investigation and prosecution of complex technology enabled crime offences
- works in partnership with the Australian law enforcement community to respond to organised and complex technology enabled crime
- actively engages in the implementation of crime prevention strategies aimed at raising awareness of cyber security risks in the Australian community, and
- cooperates with international agencies to investigate and prosecute technology enabled crime and address cyber crime issues.

AFP is a member agency of the JOA.

The **Australian Security Intelligence Organisation's** (ASIO) responsibilities are defined by the *Australian Security Intelligence Organisation Act 1979* and, in relation to cyber security, include:

- investigating electronic attacks conducted for purpose of espionage, sabotage, terrorism or other forms of politically motivated violence, attacks on the defence system and other matters that fall under the heads of security in the *ASIO Act*
- collecting intelligence both domestically and internationally on such matters, assessing the capabilities and intentions of persons and groups of security interest
- contributing to the investigation of computer network operations directed against Australia's national interests, including those targeting government and critical infrastructure assets
- producing threat assessments and protective security advice for government and critical infrastructure, and
- liaising with business on behalf of the Australian intelligence community through the Business Liaison Unit.

ASIO is a member agency of the JOA.

The **Defence Signals Directorate** (DSD) is the national authority on the security of ICT across government. DSD provides a range of information security services to ensure that sensitive government electronic information systems are not susceptible to unauthorised access, compromise or disruption. Pursuant to the *Intelligence Services Act 2001*, DSD's functions include:

- providing material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means, and
- providing assistance to Commonwealth, State and Territory authorities in relation to cryptography and communications technologies.

DSD, through the CSOC, is responsible for maintaining a comprehensive national picture of cyber security threats, through monitoring and analysis of all information sources. It provides a central point for sharing information across government and coordinates with other agencies on response activities.

DSD is responsible for developing and maintaining the Australian Government Information and Communications Technology Security Manual (ISM).

DSD is a member agency of the JOA.

The **Department of Broadband, Communications and the Digital Economy** (DBCDE) has responsibility for creating an environment that supports Australians in taking full advantage of the opportunities offered by the digital economy by:

- working with the Internet industry and the community to raise awareness of cyber security risks with a view to improving their online practices and behaviours
- working with the ISPs to enhance the security of their subscribers, including through the development of codes of practice
- working across the BCDE portfolio to promote the alignment of activities that have cyber security synergies with whole of government cyber security policy objectives, and
- collaborating internationally to address cyber security issues, ensuring that DBCDE international activities align with whole of government objectives.

The Department of Finance and Deregulation's **Australian Government Information Management Office** (AGIMO) works with Australian Government agencies to ensure the productive application of information and communication technologies (ICT). It contributes to cyber security objectives by:

- ensuring that Australian Government ICT proposals have adequately considered cyber security risks
- working with agencies to adopt a whole of government approach to the management of common assets and data sharing
- promoting security and resilience as essential requirements of e-government initiatives
- developing whole of government strategies to help meet shortfalls in skilled cyber security practitioners, and
- coordinating a strategy for managed Internet gateways for Australian Government agencies.

The **Joint Operating Arrangements** (JOA) were established by the Australian Government whereby operational cyber security agencies (DSD, AFP and ASIO) identify, analyse and respond to cyber events of serious national consequence. The JOA agencies determine which agency has primary carriage of a security event response on the basis of the nature of the event and individual agency responsibilities. It is intended that this process will be undertaken within the CSOC, drawing upon its capabilities and the staff embedded within it from relevant Australian Government agencies.

The **Cyber Security Policy and Coordination (CSPC) Committee** is the Australian Government interdepartmental committee that coordinates the development of cyber security policy for the Australian Government. The CSPC Committee:

- provides whole of government strategic leadership on cyber security
- determines priorities for the Australian Government
- coordinates the response to cyber security events, noting that its coordination and policy functions do not extend to the oversight of operations, and
- coordinates Australian Government cyber security policy internationally.

www.ag.gov.au/cybersecurity