

# **E-SECURITY REVIEW 2008**

## **DISCUSSION PAPER FOR PUBLIC CONSULTATION**

### **1. Introduction**

Australia's national security and economic and social well-being rely upon the use and availability of a range of Information and Communications Technology (ICT). Such systems include desktop computers, the Internet, mobile communication devices and other computer networks. As these systems and technologies become more pervasive, government, business and individuals are becoming more dependent on them for a range of purposes. Whether it is transacting on-line to purchase goods or services, communicating with others, managing finances, searching for information, or controlling the largest equipment in the mining or manufacturing industry, computers and computer based communications are ubiquitous. Sometimes these uses are quite clear to see. Some uses, such as the control of utilities, transport and hospital equipment and the supply of food and pharmaceuticals, are not evident to the end user.

The Australian Government understands that access to high-speed broadband services is critical to Australia's future social and economic prosperity. This is why the Government has committed up to \$4.7 billion to facilitate the roll-out of new infrastructure to provide downlink speeds of at least 12 megabits per second to 98 per cent of Australian homes and businesses. The National Broadband Network will represent the single largest investment in broadband infrastructure in Australia's history, and will further transform the way Australians communicate and do business.

A common element to all of these uses is that ICT can be used and misused in ways that were not foreseen or intended by the designers.

In Australia, organisations and individuals regularly communicate and store items of great value in electronic form. Our identities, financial details, private communications, corporate and government secrets, and our creative and academic efforts all now reside within and travel through our ICT systems. Unfortunately, as the quantity and value of the content has increased so too have the efforts of criminals and other malicious actors, who have begun to turn to the Internet as a more anonymous, convenient and profitable way of carrying out their activities. It is also a fact that attacks on critical computer systems in both the government and private sectors are being contemplated as an alternative way of conducting warfare and a way for criminals, terrorist groups and hostile intelligence agencies to damage national interests.

The Australian Government will seek to address this growth in the digital economy and the risks and threats it poses to Australia and its interests by developing an E-Security Framework. It is essential that this Framework complement other related policies for protective security and the online environment. For example, the Cyber-safety Policy is aimed at protecting individuals, especially children, from offensive content, bullying and stalking online, while the National Identity Security Strategy aims to maximise the effectiveness and interoperability of work across all governments to combat the misuse of stolen or assumed identities. The Framework must go beyond the technology itself and recognise the complexities of the purpose and usefulness of the technology, the markets and homes in which it is used, as well as its international reach.

## 2. Background

The current Australian Government approach to e-security is informed by the E-Security National Agenda (ESNA), which was established in 2001 and reviewed in 2006.

The 2006 review led to a \$73.6 million, multi-agency policy initiative, announced in the 2007-08 Budget, driven in response to increased risks in the online environment. Its three main objectives are to:

- reduce the e-security risk to Australian Government ICT systems
- reduce the e-security risk to Australia's national critical infrastructure, and
- enhance the protection of home users and small and medium enterprises from electronic attacks and fraud.

The Attorney-General's Department coordinates the Australian Government's e-security arrangements. This coordination occurs principally through the E-Security Policy and Coordination (ESPaC) committee, which includes the following agencies:

- Attorney-General's Department (Chair)
- Department of Broadband, Communications and the Digital Economy
- Australian Federal Police
- Department of Defence
- Defence Signals Directorate
- Australian Communications and Media Authority
- Australian Government Information Management Office
- Department of Infrastructure, Transport, Regional Development and Local Government
- Australian Security Intelligence Organisation, and
- Department of the Prime Minister and Cabinet.

The Australian Government considers that a new approach to e-security is required which considers Australia's readiness to deal with changing circumstances, such as:

- an increasingly hostile online security environment and emerging threats, which do not respect traditional jurisdictional boundaries; and
- the rapid and ongoing evolution of Australia's information and communications environment, including the forthcoming rollout of the National Broadband Network.

In conducting the review, current arrangements implemented under ESNA will be evaluated in light of the rapidly evolving environment and incorporated, as appropriate, in the new E-Security Framework.

### 3. Review Terms of Reference

The Attorney-General's Department is to lead a review of the Australian Government's e-security policy, programs and capabilities, assisted by other agencies represented on the E-Security Policy and Coordination Committee. The review will take account of both the threat from electronic intrusions into Australian networks and the threat from complementary attacks on their physical, administrative or personnel security arrangements.

The purpose of the review is to develop a new Australian Government E-Security Framework in order to create a secure and trusted electronic operating environment for both the public and private sectors.

The review will:

1. develop a new Australian Government policy framework for e-security, covering the span of e-security issues across government, business and the community
2. examine current programs, arrangements and agency capabilities and capacities that contribute to e-security, including:
  - a) those being implemented by agencies under the E-Security National Agenda
  - b) incident response and crisis management arrangements for e-security, including the recommendations from Australia's participation in Exercise Cyber Storm II, and
  - c) other relevant information and communications technologies (ICT) initiatives being undertaken by the Commonwealth and by state and territory governmentsto establish their suitability and effectiveness to achieve the policy objectives of the new Framework.
3. address emerging e-security issues including:
  - a) those resulting from technological change, including roll-out of the National Broadband Network, and
  - b) an increasingly hostile online security environment, which does not respect traditional jurisdictional boundaries
4. consider opportunities provided by international cooperation, including engagement with similar economies and like-minded governments
5. bring forward recommendations, prioritised in accordance with an assessment of risk, for consideration by Government to:
  - a) tailor programs and agency capabilities and capacity to achieve the policy objectives of the new Framework
  - b) address current and emerging threats, and
  - c) determine how to measure the success of each approach
6. principally focus on measures to be effective in the period to mid-2011, but also take into account longer term considerations, and
7. consult with relevant stakeholders and experts in government, business, academia and the community

The review is to be completed for Government consideration by October 2008.

An executive committee comprising senior representatives of the Attorney-General's Department, the Defence Signals Directorate, ASIO, the Department of the Prime Minister and Cabinet, the Department of Broadband, Communications and the Digital Economy, the Australian Federal Police and the Australian Government Information Management Office will provide oversight of the Review.

## 4. Framework

The Australian Government aims to create a secure and trusted electronic operating environment for all Australians. The purpose of the review is to develop a new Australian Government E-Security Framework. This outcome can only be achieved through cooperation between all levels of government, strong partnerships with Australian industry and outreach to the education sector and the broader community.

For the purposes of consultation, the review will examine issues specific to the following sectors of the community:

- **Government** (all levels)
- **Business** (including critical infrastructure, ICT vendors and service providers)
- **Education** (including skills development and protection of ICT infrastructure)
- **Home Users & Small Business**

The Government recognises that the security of each of these sectors is often influenced, both positively and negatively, by the policies and practices of the others. In recognition of these inter-dependencies, the framework will acknowledge the differing role that the Government has in supporting each sector.

The review is particularly interested in your views on the respective roles and responsibilities of these different sectors, and how they can best be integrated within the national framework.

## 5. Capabilities and Enablers

In making your submission, the review suggests that you address one or more of the following areas of interest. These relate to capabilities that shape and influence the e-security environment, and may apply differently to each of the sectors. They include:

- Secure and safe online behaviour
- Secure information exchange
- Assurance of products and systems
- Threat awareness, detection and mitigation
- Prevention, investigation and prosecution of cyber-crime
- Crisis management and coordination

In addressing each of these capabilities, the review encourages you to consider the role of the following key enablers:

- Supporting policies, procedures and technical standards
- Education, training and awareness raising
- Information sharing, including international cooperation

- Ongoing testing, evaluation and exercises
- Research and development
- Legal and law enforcement
- Physical, administrative and personnel security

You do not need to address all the areas listed above in your submission and you may comment on any other issues that you consider relevant to the terms of reference.

The following questions may also assist you in writing your submission:

- What do you see as being Australia's top three e-security priorities?
- What do you believe are the respective roles and responsibilities of government (including State/Territory and local), industry and home users in addressing e-security issues?
- In what ways could Australia better protect itself against e-security threats and vulnerabilities?
- What do you consider to be your role in e-security in Australia?

## **6. Submissions**

The Australian Government is seeking written submissions on the issues raised in this discussion paper from the business community and members of the public with an interest in e-security. The closing date for submissions is 31 July 2008. Written submissions should be forwarded to:

Email: [e-securityreview@ag.gov.au](mailto:e-securityreview@ag.gov.au)

Mail: E-Security Review Team  
Attorney-General's Department  
Robert Garran Offices  
National Circuit  
BARTON ACT 2600

Fax: 02 6272 7190

Submissions should identify the name of the party making the submission, the organisation they represent (where relevant), as well as contact details.

All submissions will be treated as public unless the submitter specifically requests that the submission—or part thereof—be handled in confidence. Email disclaimers will not be considered sufficient confidentiality requests. The Government also reserves the right not to publish any submission, or part of a submission, which in the view of the Government contains potentially defamatory material. Note that submissions or comments will generally be subject to freedom of information provisions.

Enquiries relating to the submission process may be directed to 02 6272 7111 or by email to [e-securityreview@ag.gov.au](mailto:e-securityreview@ag.gov.au) (preferred).