



Australian Government

# E-Security

## National Agenda



## Background

Recognising the increasing reliance of government, business and home users on information and communications technologies (ICT), the Australian Government established the E-Security National Agenda (ESNA) in 2001 to create a secure and trusted electronic operating environment for both the public and private sectors.

Since then, the e-security landscape has changed significantly with the emergence of sophisticated, targeted and malicious online attacks. These attacks potentially come from a number of sources, including organised crime, foreign intelligence services and politically motivated groups that pose a risk to the:

- continuity of government
- reliable delivery of critical services by both the public and private sector, and
- identity and financial information of home users and small- to medium-sized enterprises (SMEs).



## ESNA Review

In 2006, the Attorney-General, the Minister for Communications, Information Technology and the Arts, the Minister for Defence and the Special Minister for State announced a review of the ESNA to ensure that Australia's policy and operational framework continues to be responsive to the changing e-security environment.

The review found that because the online environment is highly interconnected, e-security threats to different segments of the Australian economy cannot be addressed in isolation. This key finding saw the development of three new priorities to address concerns and to assist in achieving the original objective of ESNA, to:

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

In May 2007, the Government announced funding of \$73.6 million over four years for new measures to address these three priorities.

## Operational Arrangements

Below is a brief description of the role and responsibilities of relevant Australian Government agencies as they align to the three priorities.



## Priority One:

### Reducing the e-security risk to Australian Government information and communications systems

#### Defence Signals Directorate

As Australian Government agencies have significantly increased the range of services delivered online since the ESNA was first established, the risks associated with the Internet have also grown rapidly. Respecting and protecting the privacy and information security of citizens, businesses, communities and organisations has become a key focus of government activities.

In an increasingly complex and technically challenging e-security environment, the Defence Signals Directorate's (DSD) ability to provide assistance to government agencies in securing their networks and systems will be enhanced. In particular, DSD will deliver an advanced capability to defend the Government's computer networks, with an emphasis on the protection of proprietary information, national security matters and private and confidential information about members of the Australian public.

#### Department of Finance and Administration (Australian Government Information Management Office)

Like other parts of the Australian economy, the Government has embraced Information and Communications Technology (ICT) to improve the productivity, efficiency and reach of its services. To minimise the risk of disruption to government services arising from e-security incidents, the Government must have a robust e-security strategy in place.

The Department of Finance and Administration's Australian Government Information Management Office will establish a single framework for the continued delivery of government services in the event of a disruption and/or failure of government-operated ICT.

## Priority Two:

### Reducing the e-security risk to Australia's national critical infrastructure

#### Attorney-General's Department

The national information infrastructure is the information system that underpins critical infrastructure. The majority of Australia's critical infrastructure is owned and operated by the private sector. Although critical infrastructure organisations usually have advanced risk management strategies in place to manage e-security incidents and ensure business continuity, the consequences of a severe e-security incident can be of national significance.

The Attorney-General's Department (AGD) will expand the Australian Government Computer Emergency Readiness Team (GovCERT.au) to provide owners and operators of Australia's critical infrastructure with information to help reduce the risks from sophisticated electronic attack, and to provide government with information about the electronic risks to critical infrastructure. AGD will conduct a feasibility study into the development of a business centre that allows security information to be shared quickly between government and critical infrastructure organisations, minimising the impact of electronic attacks. AGD will also prepare for electronic incidents affecting critical infrastructure by coordinating and undertaking cyber-exercises, including Australia's participation in international cyber-exercises such as Cyber Storm.

#### Australian Federal Police

A strong and effective law enforcement capability is a vital component of the Government's ability to protect the National Information Infrastructure (NII) and to provide a secure and trusted electronic operating environment to protect Australia's interests nationally and internationally.

The Australian Federal Police (AFP) will deliver this law enforcement capability through enhanced investigative and technical capabilities targeting

criminal threats to the NII. It will continue to support Australia's e-security through national and international initiatives in Asia and the Pacific regions. This will increase the AFP's effectiveness in combating online criminal activity, including enhancing its ability to detect, deter and investigate criminal threats to the NII.

### Priority Three:

#### Enhancing the protection of home users and SMEs from electronic attacks and fraud

##### Department of Communications, Information Technology and the Arts

Home users and SMEs are increasingly reliant on online technologies in their every day lives, whether it be for banking, shopping, exchanging information or using government services. However, many home users and SMEs either do not have an appreciation of e-security risks or are unaware of what they can do to improve their online security. Raising the awareness of home users and SMEs about e-security issues is a vital step in reducing their overall exposure to e-security threats.

The Department of Communications, Information Technology and the Arts (DCITA) aims to raise the awareness of home users and SMEs by providing them with the knowledge and skills to improve their computer defences and their online behaviours. The primary mechanism for disseminating information will be the Government's e-security web site [www.staysmartonline.gov.au](http://www.staysmartonline.gov.au). DCITA will also develop information resources to help schools educate students and their families about secure online practices.

##### Australian Communications and Media Authority

Networks of compromised computers of home users and small businesses are being used to send malicious spam, launch 'denial of service' attacks and steal personal and financial information.

The Australian Communications and Media Authority will extend its work with Australian internet service providers to help identify compromised computers belonging to Australian home users and SMEs so the providers can then assist the computers owners in rectifying the problem.

### Administrative Arrangements

The Review found that the whole-of-government arrangements needed to reflect the changes in the e-security environment and support an integrated approach to address e-security issues across the Australian economy.

A new whole-of-government interdepartmental committee, the E-Security Policy and Coordination (ESPaC) Committee, will be established to coordinate e-security policy throughout the Australian Government. The Attorney-General's Department will chair the committee, and its membership will be comprised of representatives from the following Australian Government agencies:

- Australian Communications and Media Authority
- Australian Government Information Management Office
- Australian Federal Police
- Attorney-General's Department
- Australian Security Intelligence Organisation
- Department of Communications, IT and the Arts
- Defence Signals Directorate
- Department of Defence
- Department of Prime Minister and Cabinet, and
- Office of National Assessments.

Other Australian Government agencies will be invited to participate in the committee as observers when appropriate.

