



IMPLEMENTING A 'CULTURE OF SECURITY' IN AUSTRALIA

The *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* are being implemented in Australia primarily through a range of measures designed to promote the development of a partnership between the public and private sectors in protecting Australia's critical infrastructure. At the same time, the guidelines are seen as relevant to broader issues of e-security. While it is acknowledged that the guidelines should be read as a whole, the measures outlined below are particularly relevant to the principles of *awareness, response, ethics, risk assessment, security design and implementation, security management and reassessment*. In particular, the establishment of the Critical Infrastructure Advisory Council provides a mechanism for the continuous re-evaluation of all aspects of security by a broadly based group of experts.

The two principles not mentioned above – *responsibility* and *democracy* – do not readily lend themselves to specific implementation action but are underpinned by Australia's general laws and practices. In this regard, Australia fully endorses the comments made in the guidelines themselves about the development of a 'culture of security'. Good security requires all participants to act in a responsible manner to mitigate risks and not merely follow rules set down in a security manual.

The Australian Government is committed to protecting Australia's critical information and physical infrastructure. The Australian Government has stated that its top three priorities are national security; economic strength; and social stability. The imperative to protect Australia's Critical Infrastructure is central to all three priorities.

To develop relationships and a coordinated strategy for protecting Australia's critical infrastructure the Government established the Business-Government Task Force on Critical Infrastructure. The Task Force brought together the various owners and operators of critical infrastructure with Australian Government and State and Territory governments and agencies, and the outcomes were significant. The Task Force made a series of recommendations that have directed a program of activity in Critical Infrastructure Protection (CIP).

E-security forms a major part of the CIP agenda and is articulated through the Australian Government's objective of creating a trusted and secure electronic operating environment for both the public and private sectors. Responsibility for the E-Security National Agenda is shared between the Attorney-General and the Minister for Communications, Information Technology and the Arts.

As part of the broader CIP agenda, a number of important initiatives are now being put in place by the Attorney-General's Department, as the lead Australian Government agency for the national information infrastructure, in order to implement a stronger regime for CIP within Australia. E-security and the implementation of the *OECD Guidelines for the Security of Information Systems and Networks* form a major element of this agenda.

The Attorney-General's Department is also reviewing its own agency security plan in the light of the OECD Guidelines.

Trusted Information Sharing Network

In November 2002, the Australian Government endorsed the recommendations of the Business-Government Task Force on Critical Infrastructure. The Task Force recommendations included the establishment of a trusted information sharing network overseen by an advisory council. The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) was launched in April 2003.

While the initial driver of CIP for the States and Territories was counter-terrorism, Australian government at all levels is now committed to an 'all-hazards' approach. The TISN reflects this all-hazards approach. The Attorney-General's Department is aiming to ensure that the TISN will work closely with the National Counter-Terrorism arrangements and other government and private sector organisations to ensure the effective coordination of CIP.

The development and establishment of the TISN has required examination of a range of complex legal issues. These have included the application of, and interaction with, a range of legislative and regulatory provisions by the TISN, relating to issues such as competition, freedom of information, and stock exchange listing. The Australian Government has developed Terms of Reference and a Deed of Confidentiality to ensure that information shared within the TISN is appropriately dealt with in a manner that ensures the maintenance of confidentiality of that information.

Critical Infrastructure Advisory Council (CIAC)

The Critical Infrastructure Advisory Council CIAC reports to the Attorney-General on the national approach to CIP. It comprises representatives from each of the Infrastructure Assurance Advisory Groups (IAAGs); each of the States and Territories; relevant Australian Government agencies; and the NCTC. The CIAC is chaired by the Attorney-General's Department. The CIAC is concerned with the medium to long-term preventive aspects of CIP, especially those issues that have cross-sector implications. It will also provide a conduit to identify requirements for CIP research.

The inaugural meeting of the CIAC was held on 27 August 2003. All current members of the CIAC were represented. The Terms of Reference and Deed of Confidentiality for the CIAC were discussed at the inaugural meeting and are expected to be ratified by the CIAC members out of session during this month. The next meeting of the CIAC will be held on 4 December 2003.

Infrastructure Assurance Advisory Groups (IAAGs)

The TISN includes a number of Infrastructure Assurance Advisory Groups (IAAGs) from different industry sectors. IAAGs for the water services, communications, food chain, banking and finance, energy and health have been formed. Each of the IAAG sectors will be represented on the CIAC.

The Australian Government hopes that the IAAGs will establish links with their equivalent bodies overseas, for example the US Information Sharing and Analysis Centres (ISACs). Australia has also been holding bilateral and multilateral talks with the United States, Canada, Japan, New Zealand and the United Kingdom on critical infrastructure protection. This type of cooperation between nations will help counter threats and vulnerabilities and will, in turn, have a positive flow-on effect to all economies involved.

Expert Advisory Groups

A number of Expert Advisory Groups are also expected to be established as the TISN matures. These groups will consist of academics and sector experts and will research and/or analyse specific issues as required. These groups will be established by the CIAC.

CIP National Strategy

The CIAC is currently considering a draft National Strategy for CIP, developed by the Attorney-General's Department, which provides an overarching statement of principles, strategies and responsibilities for CIP in Australia from an 'all hazards' perspective. The strategy recognises the relationship between CIP and a significant number of strategies, plans and procedures already existing to deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies. The strategy is being prepared in consultation with the CIAC, builds on the work of the National Counter-Terrorism Committee (NCTC), and is based around the Statement of Principles for CIP developed by the Attorney-General's Department.

AusCERT

To assist the broader community, the Australian Government has signed an agreement with the AusCERT, the Australian computer emergency response team (CERT) operating out of the University of Queensland, for the creation of a National Information Technology Security Reporting and Alert Scheme. This scheme, which was launched in May 2003, allows computer users to receive alerts about common computer threats and vulnerabilities, and provides a method of reporting suspected security incidents. AusCERT's wide range of information sources, including other CERTS, software and anti-virus vendors and IT research organisations from around the world, enable it to provide accurate, up-to-date and relevant alerts and warnings. AusCERT will analyse the data it collects from the scheme to determine whether there is an emerging threat or pattern of attacks to assist with prevention, detection and response to security incidents.

Regional CERT Capacity Building

The Australian Government is aware that lasting and truly secure electronic environment can only be achieved by strengthening the E-Security of all economies connected to the Internet. The Australian Government is leading efforts to enhance e-security within the region. In APEC, Australia is leading an initiative to build CERT capacity and raise awareness of the value of CERTs in developing economies, through APEC's Telecommunications and Information Working Group - APEC TEL.

With co-funding from the Australian aid agency, AusAID, the Attorney-General's Department is coordinating a CERT Capacity Building Project (CERT Project) taking 'in-country' CERT capacity building training to Papua New Guinea, the Philippines, Thailand, Vietnam and Indonesia.

The department also conducted seminars on CERT capacity building and awareness raising at the March and October 2003 APEC Telecommunications and Information Working Group meetings which were open to all APEC Economies.

The CERT project also funds the development of guidelines for establishing CERTs and provides funding for a CERT communications network to allow regional CERTs to exchange alerts and advisories. In addition, Australia is overseeing an APEC funded project to allow in-country CERT training to be provided to Chile, Peru, Mexico and the Russian Federation.

The objective of these closely linked projects will be the creation of a network of CERTs throughout the Asia/Pacific region which will be able to exchange information on IT security issues quickly and securely.

Australian Hi-Tech Crime Centre

On 5 November 2002, the Australasian Police Ministers' Council agreed that the Australian Federal Police (AFP) would host an Australian Hi-Tech Crime Centre (AHTCC). The Centre provides a coordinated national approach to combating serious and complex hi-tech crime, while helping to improve States and Territories capacity to deal with e-crime. The AHTCC is being funded and staffed by the Commonwealth and the states and territories. In the May 2003 Budget, the Commonwealth announced additional funding to further enhance the AFP's e-crime investigative capacities.

The AHTCC acts as a hub to assist the AFP's international liaison network and Australia's mutual assistance agreements for dealing with international crime. It coordinates investigations of attacks on critical infrastructures with domestic State law enforcement agencies, relevant Australian Government agencies, and overseas agencies such as Interpol, the FBI and Britain's Hi-Tech Crime Unit.

Cybercrime Legislation

In 2001, the Australian Government introduced new computer crime legislation, the *Cybercrime Act 2001*. This was an important step toward achieving national consistency with the Council of Europe Cybercrime Convention and remedying deficiencies in existing laws. The computer offences are designed to protect the security, integrity and reliability of computer data and electronic communications. The offences provide a strong deterrent to persons who engage in cybercrime activities such as hacking, computer virus propagation and denial of service attacks. The legislation also includes enhancement of law enforcement powers relating to the search and seizure of electronically stored data and will strengthen business and community confidence in new technologies by ensuring that criminal misuse of those technologies is penalised. In response to heightened awareness of the potential for cyber-terrorism, the government has also introduced *Security Legislation Amendment (Terrorism) Act 2002* which makes specific reference to the concept of cyber-terrorism, the action or threat of action seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to information and telecommunications systems.

IT Evidence Handbook

The Attorney-General's Department is also continuing its efforts to raise the awareness of CIP issues with stakeholders. These efforts include the launching of the *Guidelines for the Management of IT Evidence* (Handbook 171) in August 2003 as part of the E-Security National Agenda. The handbook provides a statement of best practice to assist businesses and law enforcement agencies to improve their methods for collecting and preserving evidence in digital form and making it available for evidentiary purposes in civil, administrative or criminal legal proceedings. The handbook provides a 'learned text' that can be used in civil litigation, will encourage businesses to seek damages for breaches of IT security, and become a driver for better IT security.

National Research Priorities and Safeguarding Australia

In December 2002, the Prime Minister announced that the Australian Government had selected four National Research Priorities to focus Australia's investment on research. One of the four priorities, 'Safeguarding Australia', includes protecting Australia's critical infrastructure, particularly computing systems. Develop a critical mass of research in e-security is an essential part of this priority goal.

The Attorney-General's Department, in concert with the broad range of other Australian Government departments and agencies with responsibilities for CIP, is seeking to strengthen relationships between the Australian research community and the owners and operators of the nation's critical infrastructure. The TISN will assist in the implementation of the 'Safeguarding Australia' priority by acting as a conduit to identify requirements for CIP research and by advising the Australian Government of the relevance of research proposals.

Future Directions

Establishment of the TISN is an important step in building an effective partnership between government and private sector owners and operators of critical infrastructure. In particular, the TISN now provides a forum for the private sector to raise issues or matters of concerns that relate to CIP. Accordingly, it is important to ensure that the Australian Government has in place the capabilities to respond effectively to the threats and vulnerabilities that are identified through the partnership. In addition, the Australian Government needs to reciprocate the efforts by the private sector to add value to the sharing of information to protect critical infrastructure.

In this regard, the Attorney-General's Department, in concert with the broad range of other Australian Government departments and agencies with responsibilities for critical infrastructure protection, is examining a number of measures to strengthen the TISN. These future directions have been identified against the six key proposals in the Business-Government Task Force Report on Critical Infrastructure adopted by the Australian Government in November 2002. These measures will complement the National E-Security Agenda and assist the development and promotion of a "culture of security".

Peter Ford
A/g Deputy Secretary

Telephone: 6250 6654
Facsimile: 6250 5945
Email: peter.ford@ag.gov.au