SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS
ATTORNEY-GENERAL'S DEPARTMENT

Sub Program 2.1.1

Question No. 183

Senator Williams asked the following question at the hearing on 25-27 May 2009:

In relation to cyber-security;

a) In light of the U.S.President's release of the Government plans to install a "cyber security czar" to oversee the protection of the US national digital assets, what is the Federal Government's plans, and will we give the protection of Australia's Digital Assets the same level of attention,
b) what are Australia's strategic cyber priorities and how is Australia pushing, or will push, for partnership with the US to pursue international aspects,
c) how will Australia use cyber security requirements to improve benefits from best practices efforts, and
d) what is Australia doing to promote a robust International Watch and Warning Network, to strategically target malicious actors and enablers?

The answer to the honourable senator's question is as follows:

a) The Australian Government has a comprehensive range of programs to respond to e-security threats.

As announced in the 2009-10 Budget, the Government is creating a new Australian Government national computer emergency response team (national CERT). The national CERT will provide a single point of contact for e-security information for all Australians and Australian business.

The national CERT will include the current Australian Government Computer Emergency Readiness Team (GovCERT.au), which is part of the Attorney-General's Department. GovCERT.au assists the owners and operators of Australia's critical infrastructure and key businesses - including our 'digital assets' - to secure their electronic systems. This includes the communication of sensitive electronic threat information to these organisations, liaison and coordination with foreign governments on cyber security issues and assistance with the coordination of Government policy for computer emergency prevention, preparedness, response and recovery.

The national CERT will complement the new Cyber Security Operations Centre (CSOC) within the Department of Defence, announced in the Defence White Paper. The CSOC will provide the Australian Government with increased situational awareness and coordinate response to cyber security incidents of national importance.

Australia has well established business-government partnerships in the area of critical infrastructure protection. The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is a forum for the sharing of general security threat and vulnerability information, between businesses, and between government and business.

b) The Australia Government's e-security aim is the maintenance of a secure and trusted electronic operating environment for both the public and private sectors.

Australia has strong relationships with the United States, regional partners and key allies and is active in multilateral fora on e-security issues. These relationships are supported by joint critical infrastructure protection partnership arrangements focused on e-security matters.

The E-Security Review 2008 recognised the importance of building international partnerships on e-security to promote awareness, marshal expertise and eliminate safe havens for cyber criminals.

c) The Australian Government has a range of initiatives in place to promote e-security best practice in both the public and private sectors.

Australian Government agencies are required by the Australian Government Protective Security Manual to comply with the Information Security Manual (ISM) for the protection of official government information when it is processed, stored or communicated by Australian Government systems.

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is a forum for the sharing of general security threat and vulnerability information, between businesses, and between government and business, including the identification and promotion of best practice.

The Australian Government Computer Emergency Readiness Team (GovCERT.au) assists critical infrastructure and key businesses to help them secure their electronic systems. GovCERT.au has recently established Information Exchanges to assist with this process.

The Department of Broadband, Communications and the Digital Economy undertakes a number of initiatives to enhance the protection of home users and small business from electronic attacks and fraud.

d) Australia actively promotes global preparedness for cyber attack through its participation in multilateral fora including the International Watch and Warning Network (IWWN). The E-Security Policy and Coordination Branch of the Attorney-General's Department assists in the coordination of, and participates in, IWWN member exercises and activities and is strongly engaged internationally on e-security matters.

The Australian Government Computer Emergency Readiness Team (GovCERT.au) maintains close ties with foreign governments and their computer emergency response teams (CERTs) – including for sharing e-security threat information.

The Australian Government participates in a range of exercises that test the working relationships between Australia and international partners.