DEPARTMENT OF DEFENCE SUBMISSION TO THE HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON COMMUNICATIONS

INQUIRY INTO CYBER CRIME

The Department of Defence assists the Australian Government in the protection of their information against the cyber threat and in its submission below has provided answers about this role that address the terms of reference proposed by the committee.

The organisation in Defence that assists the Australian Government in the protection of its information is the Defence Signals Directorate (DSD). DSD is the national authority for information security for the Australian Government and provides material, advice and 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, in accordance with section 7 (c) of the *Intelligence Services Act 2001*.

DSD also provides support to non-government critical infrastructure, but only through its relationships with the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and the Attorney-General's Department (AGD).

DSD works with ASIO and AFP to protect the National Information Infrastructure (NII) under the Joint Operating Arrangements (JOA) which was put in place in 2000. Under these arrangements each agency brings different expertise to respond to critical incidents involving the NII. AGD is the lead agency for e-security policy and, while not a formal part of the JOA, it acts in an advisory and liaison capacity between the JOA and the private sector on matters relating to the protection of information of national interest.

DSD's information security capability has been significantly enhanced by funding under the White Paper that has built on previous proposals such as the E-Security National Agenda (ESNA).

The Defence White Paper released in May 2009, identifies cyber operations as a critical component of Australia's defensive capability. A Cyber Security Operations Centre will become the new frontline under the White Paper initiative to provide better situational awareness and the ability to facilitate responses to cyber security incidents.

The new Cyber Security Operations Centre will be staffed by skilled experts to maximise the Government's ability to detect and rapidly respond to fast-evolving and aggressive cyber attacks.

It will do this by drawing on an array of sources in the intelligence, law enforcement and industry communities to provide a comprehensive picture of threats to Australian information and systems. It will also act as a coordination point for responses by Government agencies and will work in close collaboration with overseas partners.

Defence's answers to the terms of reference

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans

Over the last five years, government, business, industry, academia and the community have become increasingly reliant on the Internet to conduct business. While it is a simple, cost effective and efficient way to do business, it is not without risk.

Any electronic system, be it a computer, mobile phone, personal digital assistant, an industrial control system, or any other network-capable device, connected to the Internet is more susceptible to a range of threats. Connecting systems and/or devices to the Internet provides a potential opportunity for foreign intelligence services, organised crime syndicates, political activists and individuals acting alone, to exploit vulnerabilities that can facilitate access to sensitive information that was previously difficult to obtain. This includes information that would not normally be transmitted beyond an organisation, such as drafts of internal correspondence, speeches, policies, strategic plans, research, personal and business financial details and intellectual property.

b) The implications of these risks on the wider economy, including the growing economic and security impact of botnets

Defence is unable to provide expert comment on the economic consequence of the risks from botnets.

However, Defence can provide information on the security impact of botnets to government networks that it has seen through its incident response capability.

A botnet is a collection of many computers that are under the control of a single entity and can be used for malicious purposes. Botnets did play a role in the cyber attacks against Estonia and Georgia in 2007 and 2008.

DSD is aware of a small number of reported instances where government agencies have been compromised by a botnet and remediated the situation. DSD believes that the reason why only a small number of agencies have been affected is because of good security practices as detailed under the Australian Government Information and Communications Technology Security Manual (ISM – formerly known as ACSI 33).

c) Level of understanding and awareness of e-security risks within the Australian community

Defence is unable to provide expert comment on the level and understanding of e-security risks within the Australian community.

However, it was recognised under both ESNA and the E-Security review that DSD plays a role in educating government about the cyber threat and the organisation received funding under ESNA to educate and raise awareness across government about the e-security risks.

d) Measures currently deployed to mitigate e-security risk faced by Australian consumers:

- **a. Education initiatives**
- **b. Legislative and regulatory initiatives**
- **c. Cross-portfolio and inter-jurisdictional coordination**
- **d. International cooperation**

Defence is unable to provide expert comment on these issues.

However, DSD received funding under ESNA to educate and raise awareness across government about the e-security risks.

DSD works with ASIO and AFP to protect the NII under the JOA which was put in place in 2000. Under these arrangements each agency brings different expertise to respond to critical incidents involving the NII. AGD is the lead agency for e-security policy and, while not a formal part of the JOA, it acts in an advisory and liaison capacity between the JOA and the private sector on matters relating to the protection of systems of national interest.

e) Future initiatives that will further mitigate the risks to Australian Internet users

Defence White Paper

Under the Defence White Paper 2009 – Defending Australia in the Asia Pacific Century: Force 2030, a Cyber Security Operations Centre will be established to increase situational awareness and coordinate incident response.

The Cyber Security Operations Centre will include a continuously staffed watch office and an analysis team to respond to cyber threats in a timely manner. While this capability will reside in Defence and be available to provide cyber warfare support to ADF operations, it will be purpose designed to serve broader national security goals. This includes assisting responses to cyber incidents across government and critical private sector systems and infrastructure.

Joint Operating Arrangements

DSD works with ASIO and AFP to protect the NII under the JOA which was put in place in 2000. Under these arrangements each agency brings different expertise to respond to critical incidents involving the NII. AGD is the lead agency for e-security policy and while not a formal part of the JOA it acts in an advisory and liaison capacity between the JOA and the private sector on matters relating to the protection of systems of national interest.

National Computer Emergency Response Team (CERT)

The National CERT located in the AGD will provide a single point of contact for e-security information for all Australians and Australian businesses.
It will ensure Australian Internet users have access to information on e-security threats,

vulnerabilities in their systems and information on how to better protect their information technology environment.

The National CERT will complement the new Cyber Security Operations Centre.

f) Emerging technologies to combat these risks

Defence is unable to provide expert comment on these issues.