Symantec Australia
Submission to the Parliamentary Joint Committee of Public Accounts and Audit Inquiry Into Management and Integrity of Electronic Information in the Commonwealth

Symantec Australia welcomes the opportunity to contribute to this enquiry as part of our commitment to work with government and industry to make the global computing infrastructure safe and secure.

This submission focuses on:

- Symantec in Australia
- Assessing Threats to Government e-security
- Developing a Culture of Security
- Security At All Levels

For further information about the contents of this submission, please contact:

John Donovan
Managing Director
Symantec Australia
Level 2, 1 Julius Avenue
North Ryde NSW 2113
Ph: + 61 2 8879 1105
email: jdonovan@symantec.com

or

Mina Silvestre
Government Relations
Symantec Australia
Level 2, 1 Julius Avenue
North Ryde NSW 2113
Ph: + 61 2 8879 1008
email: msilvest@symantec.com

1. About Symantec

Symantec is the world leader in Internet security technology[1]. We provide a wide range of security solutions to companies, government agencies and individuals around the world, including virus protection, firewall and virtual private networks, vulnerability assessment and management, intrusion detection, Internet content and e-mail filtering, remote management technologies and managed security services.

Symantec works with government and industries worldwide to help make the global computing infrastructure safe and secure. Symantec's range of products, services and research gives it the broadest view of the security landscape. Symantec's bi-annual Internet Security Threat Report is the most comprehensive analysis of global cyber-security trends.

Headquartered in Cupertino, California, Symantec has more than 4,000 employees in 36 countries. For more information, please visit www.symantec.com.

1.1 Symantec in Australia

Symantec has more than 110 employees in Australia involved in Internet security protection strategies, research and development, customer service and support, sales and marketing.

The Asia Pacific Symantec Security Response lab opened in Sydney in 1997 to service the region. Its mission is to provide swift, global response to computer virus threats, proactively research and develop technologies that eliminate such threats, and educate the public on safe computing practices. The Sydney office also hosts a substantial Technical Support Centre with technicians and system engineers who provide local language support across Asia Pacific.

Symantec invests substantially in Australian IT research and development. This research includes antivirus research and development and research to support product development in the US. In addition, Symantec has a close working relationship with two Australian companies, PassMark and XtreamLok. Symantec has included Passmark's PerformanceTest software into our own web security solution and is currently using XtreamLok's Digital Rights Management software to reduce software piracy and ensure that Symantec's customers are receiving authentic software.

In March, 2003 Symantec launched a Security Operations Centre (SOC) in Sydney to provide Managed Security Services clients with security monitoring, management and response. Symantec's Managed Security Services practice offers a broad range of security services including monitoring and management of firewalls, intrusion detection systems, routers, VPNs, vulnerability scanners, antivirus and policy compliance to provide the most

[1] Garnter "2001 Security Software Market Share" and IDC "Worldwide Internet Security Software Market Forecast and Analysis, 2002-2006: Vendor Views"

comprehensive security solution for its managed security services customers, independent of vendor relationships.

Symantec's long-term commitment to its Australian operation and willingness to partner with Australian companies is recognised through Membership of the Federal Government's Partnership for Development (PfD) program. Symantec was also awarded Graduate Partner status in the PfD program in 2001.

Recognising the importance of collaboration in the information technology industry, Symantec is member of the Internet Industry Association, Business Software Alliance of Australia and AusCERT.

1.2 Symantec's partnership with government

Our commitment to partnership with governments internationally includes contributing expertise to government policy development, developing and delivering Internet security awareness programs and sharing information. In September 2002, President George W. Bush appointed Symantec's Global CEO and Chairman John Thompson to the National Infrastructure Advisory Committee (NIAC), to make recommendations regarding the security of the critical infrastructure of the United States. Symantec is also actively involved in the Information Sharing and Analysis Center in the United States whose role is to share, correlate, and analyse information in order to protect critical infrastructure.

In Australia, Symantec works with IT outsourcing partners, channel partners and system integrators to deliver security solutions to government agencies. Symantec is also committed to contributing its policy expertise to government, with regular liaison with government agencies including NOIE and Attorney-General's Department over security issues and strategies. For example, we distribute copies of our six-monthly global Internet Threat Report (http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&PID=9929124&EID=0) to key agencies involved in e-security.

Symantec's Australia/New Zealand Managing Director, John Donovan, was a guest speaker at the 2002 Prime Minister's Taskforce on Protection of Critical Infrastructure.

1.3 From LoveLetter to Bugbear - A Case Study in Local Security Expertise

The VBS LoveLetter worm was detected on the night of May 4, 2000.

Symantec system engineers, account managers and communications teams worked directly with the Australian Symantec Security Response team to ensure the provision of up-to-the minute information to our partners, corporate customers and industry organisations in Australia and the Asia Pacific region.

All corporate accounts were contacted directly to alert them to the coming threat, and anti-virus definitions were proactively distributed within a few hours of the virus being detected.

With Symantec's support, IT management companies like IBM were able to protect the security systems of government departments and other client organisations before Australia woke-up and went to work on May 5. Due to the overnight discovery of the virus and the quick reactions of the Symantec team in Australia and New Zealand, a great deal of damage was averted.

Since then the Australian team has been at the leading edge of the industry in the analysis and development of solutions for most of the high profile computer viruses and worms; for example the, Klez, Nimda, CodeRed and Bugbear worms were all discovered and managed in Australia.

The most recent of these was W32.Bugbear, where the Australian team discovered, analysed, named and developed fixes for this high profile worm that was most prevalent in South East Asia.

2. Assessing threats to Government e-security

The e-security challenges faced by the Commonwealth are similar to those of large enterprises as both have responsibility for the protection of their networks, corporate and personal data and critical infrastructure. The Commonwealth has additional e-security challenges due to the unique environments and different levels of security within the greater Commonwealth network.

The Commonwealth must also be prepared for the rapidly evolving cyber threats of tomorrow and build an IT continuity plan into its ongoing e-security strategy.

In July 2001, Code Red spread to 250,000 systems within six hours and the worldwide economic impact of the worm was estimated to be $2.62 billion. Code Red's spread was fast enough to foil immediate human intervention and the ramifications were huge.

In the future, we may see the emergence of hypothesized threats that use advanced scanning techniques to infect all vulnerable servers on the Internet in a matter of minutes or even seconds. Examples would include Nick Weaver's Warhol worm scenario or Silicon Defenses Flash worm theory. The Commonwealth must factor in an IT continuity plan as part of the Commonwealth's e-security strategy.

- Warhol Worms. Through advanced scanning, Warhol worms would use a list of about 50,000 sites to start an infection from and then used coordinated scanning techniques to infect the rest of the Internet. In theory, these worms could spread across the Internet and infect all vulnerable servers in less than 15 minutes.

- Flash Worms. Flash worms would operate similar to Warhol worms, but under the premise that a determined attacker could have obtained a list of all or almost all of the servers with service open to the Internet in advance of the release of the worm. Rather than 15 minutes, such an attack could infect all vulnerable servers on the Internet in less than 30 seconds.

It is very likely that we will continue to see polymorphic and metamorphic worms, but on a much more complex level. These worms will use stronger techniques for encrypting themselves and because they change their pattern every time they run, it could take days or even weeks for researchers to analyse and create cures.

We will also see an increasing number of threats specifically targeted at disabling security software. An example would be retro viruses that attack antivirus software by deleting virus definition tables or memory resident scanners.

3. Developing a culture of security

Security must be ongoing and cover physical structures, processes, technology and people.

In our view, best practice information security for governments and enterprises involves:

- Establishing security policies
- Risk assessments
- Standards, procedures, and metrics
- Security roadmap
- Selection and implementation of solutions
- Training of security professionals and employees
- Security management
- Incident response and recovery

3.1 Policies and standards

Symantec is aware of numerous guidelines issued to government agencies on e-security matters, including the Protective Security Manual and Australian Electronic Communications Security Instructions. We are also aware of the release in 2002 of "Australian government use of information and communication technology: a new governance and investment framework."

There is currently some confusion about what constitutes e-security guidelines and what are mandatory standards. Symantec believes that consistent policies and standards across government departments are needed to facilitate secure inter-agency communication.

3.2 Defence Signals Directorate Endorsed Product List

The current evaluation process for the inclusion of products on the DSD Endorsed Product List is lengthy and costly for suppliers. It is based on a long, open-ended evaluation period which can result in product technology becoming outdated even before it is included on the DSD Endorsed Product List.

3.3 Educating Employees

Many employees in today's workforce are not aware that they play an important role in their organisation's security. They download programs from the Internet, open unsolicited e-mail attachments, participate in file-swapping programs, engage in instant messaging, and neglect to update passwords and antivirus protection – all activities that could put the corporate network at risk.

Symantec has launched a comprehensive, measurable training and communications program designed for organisations to implement over the course of one year to increase employee security awareness. The program enables organisations to improve security posture by reducing information security risk posed by employees.

The Symantec Corporate Security Awareness Program provides participating organisations with materials on CD-ROMs that include recommendations for program implementation, electronic files of printed materials that can be used to internally promote and support the success of the initiative, technology-based security awareness training modules, as well as mechanisms to measure and track the participation and progress of employees. The program aims to empower all employees to take an active role in the protection of their organization's resources.

Symantec concurs with the following views on employee education on e-security as put forward in the "Australian Government Use of Information and Communication Technology:

- Agencies should ensure that staff and management know and meet their minimum obligations in relation to security.
- Each agency needs to undertake a proactive role in creating a culture of security in relation to its operations, by learning from and using the skills found throughout the government.
- Agencies need support for the creation and delivery of security training modules as part of general staff training. This applies to all new starters as well as those moving into new roles with specific security requirements.
- Senior management must take responsibility for implementing and monitoring security requirements at an agency level.
- The Australian National Audit Office should review agencies' efforts to create cultures of compliance. Such audits would raise awareness about the importance of people and process issues as well as the physical, system and software measures necessary to create a secure environment.

3.4 Private/Public Sector Co-operation in electronic security

Companies such as Symantec assist in alerting industry and government to threats, providing tools and advice on best practice for managing security threats and methods of recovery after an attack. Symantec is also very active in educating organizations and end users about security issues and prevention through Symantec Education Services and involvement in consumer activities such as National Cyber Security Day in the United States.

Symantec's Virus and Security Alert Services deliver instant notifications of the latest virus threats, and network and computer vulnerabilities to any device anywhere in the world, 24 hours a day, 7 days a week. When a new threat or vulnerability is discovered, Symantec Security Response experts provide rapid emergency response, delivering up-to-the minute information and advice so that security staff can proactively stop the threat before it impacts the network.

Alerts are sent to one wireless device, as well as a back-up email. Customers may choose to be notified of all alerts, or a sub-set, based upon the threat category level selected for each wireless device. This service was initially setup and trialled in Australia for local customers before being adopted worldwide.

Symantec has an ongoing relationship with AusCERT, often sharing information about viruses and other computer security issues. Symantec led the initiative to create the Australian Anti-virus Research Forum (AAVRF) which AusCERT hosts and chairs. This is an electronic forum where security agencies and vendors can exchange time-critical information about computer-based threats.

Symantec supports initiatives such as the National Information Security Advice Scheme pilot. We believe that Australia's critical infrastructure protection relies on ongoing input from various organisations like AusCERT as well as Internet security vendors to deliver proactive, comprehensive and timely information about the very latest security threats.

4. Security At All Levels

While this inquiry is focused on government security, it must be recognised that security lapses outside government can also pose a threat. Every personal computer with an Internet connection is an onramp to the information superhighway, and therefore a potential security threat.

Government leadership in maintaining a culture of security can set an important example to corporations and individuals about their own responsibilities.

Consumer education about simple security measures is vital to protect against online fraud and security threats.

In the United States, the National Cyber Security Alliance, a group of businesses and government organisations, including Symantec, that have aligned to educate consumers on the importance of protecting PCs from online intruders, has also chosen daylight savings as a time to encourage consumers to conduct twice-yearly checks of their home computers' security.

In the USA, Symantec has created a program to leverage National Cyber Security Day reminding consumers to check their PC security when they adjust their clocks. To make this easy, Symantec has a free Security Check service available online. We would encourage a similar Cyber Security Day to be established in Australia via collaboration between government and industry.