World e-Parliament Conference 2014

8 - 10 May 2014 // National Assembly of the Republic of Korea // Seoul
Securing Parliamentary Data

Department of Parliamentary Services, Australia
Eija Seittenranta - Chief Information Officer
Department of Parliamentary Services (DPS)

- DPS is a service department that supports the Federal Parliament of Australia.
- Principal support agency for the operations of Australian Parliament House.
- Provides various services to the four Parliamentary departments, Members, Senators and their staff.
- All ICT services for parliament in APH and the ~260 electoral offices across Australia.
• Vital part of our services is securing the data of the Parliamentary departments, Members, Senators and their staff.

• Complex environment with a vast array of user requirements and work scenarios.
Types of attacks we see attempted

- Social engineering
- Advanced Persistent Threats
- Malware
- Spamming and denial of service

- By: hackers, hactivists, criminals, nation states
Key Steps Taken to Secure Data

• Adoption of the Australian Government Information Security Manual (ISM)

• Implementation of Top 35 Strategies to Mitigate Targeted Cyber Intrusions

• Building a dedicated ICT Security team

• Improving practices and processes

• Accreditation of systems
Adoption of the ISM

• Establishes a baseline level of security for Australian public sector agencies
• It is produced by the Australian Signals Directorate (ASD)
• The manual is the standard which governs the security of Australian government ICT systems.
ASD reported that at least 85% of the targeted cyber intrusions they respond to could be prevented by following the Top 4 mitigation strategies.

The Top 4 are:

- Use Application Whitelisting to help prevent malicious software from running;
- Patch applications such as Java and Adobe Flash;
- Patch operating system vulnerabilities; and
- Restrict Administrative privileges to operating systems and applications based on user duties.
What are we concerned about for 2014-2015

- Social Media
- Advanced Persistent Threats
- Mobile related attacks
- Balancing security and usability
Questions