

Australian GovCERT.au

Protecting CIP from Cyber Threats

'it's about working together'

Greg Mazzone – Director, GovCERT.au
Attorney-General's Department

Seoul, 18 November 2009

Topics:

- GovCERT.au – Critical Infrastructure Protection
- eSecurity Review 2008 – Australian Government
- Information Exchanges – Industry and Government
- New national CERT

GovCERT.au

- Started in 2005
- Part of the Attorney-General's Department eSecurity Policy and Coordination Branch
- Part of National Security Resilience and Policy Division

GovCERT.au

- GovCERT.au coordinates Australian Government policy
 - for computer emergency preparedness, response, readiness and recovery in relation to Australia's critical infrastructure.
- GovCERT.au provides advice, information and funding
 - to help owners and operators of critical infrastructure secure their networks and systems.
- Provide Government with more informed advice about risk to specific parts of critical information systems infrastructure.

What does GovCERT.au do?

- Conducts exercises to test readiness and response
- Provide funding – CNVA, control systems training
- Provide security bulletins – vulnerabilities
- Provide briefings to private companies about sophisticated threats

eSecurity Review 2008

- Part of a two yearly process
- Another due 2010
- Due to the changing threat environment

Government Response

- ISP Code of Conduct – release December 2009
- Australian Government Cyber Security Strategy – released soon
- Information Exchanges – working with business
- New national CERT

Information Exchanges (IE's)

- Outcome of the E-Security Review 2008
- Based on forums conducted in the UK and USA
- Currently have three, covering
 - control systems (SCADA) – mainly utilities
 - telecommunications &
 - banking & finance

Information Exchanges

- A closed forum for the exchange of sensitive technical information between the Australian Government and owners and operators of critical information & infrastructure systems.
- Discussion focused on technical threats and vulnerabilities seen within and attributed across industry sectors.

A new national CERT – why?

- Outcome of the E-Security Review 2008
- Better coordinate Australia's cyber event response arrangements – Industry – States - Federal
- Provide a single POC for cyber security information domestically & internationally

New national CERT

- Incorporate a number of current activities including GovCERT.au & it's services
- Readiness → Response
- Provide Response and Coordination for Australian businesses and Community.
- Negotiating with University of Queensland (Brisbane) to have AusCERT provide some services as contractor to new new national CERT.

New national CERT

- New name – 23rd November 2009
- Limited initial capability from Jan 2010
- Full initial operations available end June 2010
- Managed by Attorney-General's Department

New national CERT

- Trusted Point of Contact in
 - Critical Information & Infrastructure (GovCERT.au)
 - Systems of National Interest (new)
 - Internet Industry Organisations (new)
- Watch this space
 - New services and products

Contact details

Contact details:

Email: govcert@ag.gov.au

Website: www.ag.gov.au/govcert

Telephone: 1300 172 499

Thank you!
Questions?