Control Systems Security: Australian Government Activities

Dr. Jason Smith
Asst. Director, Operations
CERT Australia
Attorney-General’s Department
Topics:

1. Context and aims of Australian Government activities.

2. Summary of key activities and their outcomes

3. Recent developments
Context

- Business – Government partnership required
- Information sharing and support central to strategy

- Examined the Australian Government’s cyber security policy, programs and capabilities with the aim of developing a new Australian Government policy framework for cyber security

- “...increasingly evident that the sophistication of our modern community is a source of vulnerability in itself.”
- Cyber security acknowledged as a top national security priority

Cyber Security Strategy (2009)
- Articulates the overall aim and objectives of the Australian Government’s cyber security policy
- Sets out the strategic priorities that the Australian Government will pursue to achieve these objectives.
General Aims

- Provide guidance and facilitate information sharing
- Increase comprehension of risks and access to effective mitigation strategies
- Provide operational support
INFORMATION SHARING
Trusted Information Sharing Network for Critical Infrastructure Protection

Australia’s Critical Infrastructure Protection Arrangements

National Counter-Terrorism Committee

National Committee on Critical Infrastructure Protection (NCCIP)
Federal, state and territory governments

Attorney-General

Business Government Advisory Group on National Security (BGAG)

OTHER GOVERNMENT BODIES

E-Security Policy and Coordination (ESPaC) Committee

Australian Government Senior Officers Group (AGSOG) - NCCIP

Trusted Information Sharing Network

Critical Infrastructure Advisory Council (CIAC)

Infrastructure Assurance Advisory Groups (IAAGs)

Banking & Finance (AGD)
Emergency Services (EMA)
Food Chain (DAFF)
Mass Gatherings (AGD)
Water Services (AGD)
Communications (DBCDE)
Energy (DRET)
Health (DHA)
Transport (DITRDaLG)

Expert Advisory Groups (EAGs)

CIP Futures (AGD)
IT Security (DBCDE)

Agency/portfolio shown in brackets provides support services and interface with Australian Government

Legend:
AGD: Attorney-General’s Department
EMA: Emergency Management Australia
DAFF: Department of Agriculture, Fisheries and Forestry
DBCDE: Department of Broadband, Communications and the Digital Economy
DRET: Department of Resources, Energy and Tourism
DHA: Department of Health and Ageing
DITRDaLG: Department of Infrastructure, Transport, Regional Development and Local Government

December 2007
Commissions development of guideline documents for owners and operators of CI

http://www.tisn.gov.au

- SCADA Security Advice for CEOs
- Infrastructure information in the public domain – a guide to mitigating security risks
- Risk Management Framework for SCADA
- Diesel Fuel and Backup Generators – Issues for CEOs and Risk Managers
- etc
SCADA Community of Interest (CoI):

- A Working Group of the ITSEAG
- Peer to Peer and cross sector network
- Meets quarterly
  - Issues of common interest
  - Relationships for cross organisational & international incident responses
  - Program of work to develop a resilience framework
SCADA Practitioner / Vendor Forum:

- Hosted by Government 2008 and 2009

- Invitation only – SCADA practitioner inviting one or more of their vendors

- Promote better understanding of practitioner needs / vendor constraints
  - Key message from vendors “If you don’t demand security, we will not provide it”
RISKS AND MITIGATIONS
Risks and Mitigations

- Critical Infrastructure Protection Modeling and Analysis (CIPMA)
- Computer Network Vulnerability Assessment (CNVA)
- Cyberstorm Exercises
- National Security Science and Technology (NSST) Research Support for National Security (RSNS) Program
- Idaho National Labs Advanced Cyber Security Training and Workshop
World leading computer modelling activity commenced in 2004

Funded $AUD16 Million / 4 years (to 2013)

Models and examines complex relationships and interdependencies in critical infrastructure

Five sectors currently engaged
- Banking and finance
- Communications
- Energy
- Water services
- Transport
Strong business-government partnership:

- Modelling and analysis of potential tsunami impacts → oil and gas pipeline redesign for increased resilience.

- Modelling and analysis used to expose interdependencies and inform business continuity management exercise construction.
Grants scheme:

– commenced in 2005

– subsidies to critical infrastructure organisations, including GBEs

– to undertake independent assessments of their critical ICT networks and systems, including process control systems.

– 32 Assessments, total cost AUD$4.4Million
Computer Network Vulnerability Assessments

- Energy
- Water Services
- Transport
- Health
- Banking & Finance
- Food Chain
- Defence industry
Cyber Storm Exercises

- Large scale cyber security exercise sponsored by U.S. DHS.

- March 2008 CSII
  - 56 Australian organisations (across government and business) involved
  - International involvement by US, UK, NZ, Canada

- Late September 2010 CSIII
  - Australia participating
  - International Watch and Warning Network (IWWN) also participating
National Security Science and Technology (NSST) Research Support for National Security (RSNS)

- Administered by the Department of the Prime Minister and Cabinet

- Support short-term requirements while developing long-term capabilities

- Exemplar projects since 2007
  - Incident response in control systems environments
  - A general forensic model for process control and SCADA systems
  - Critical infrastructure resilience: an ICT governance approach
  - Forensic readiness for control systems
INL Advanced Cyber Security Training

Hosted by DHS Control System Security Program

- 5 day program
- provides intensive hands-on training for the protection and securing of control systems from cyber attacks
- Based on a red-team / blue-team exercise
- Conducted within an actual control systems environment
INL Advanced Cyber Security Training

- Australian Government provides a grant of up to $AUD5000
- Delegations sent in 2007, 2008, and 2009
- Australia-only event held in November 2009
- Approximately 60 people from industry have attended so far
OPERATIONAL SUPPORT
Current Arrangements

Cyber Security Strategy:

- released November 2009

- outcome of the E-Security review 2008

- details government objectives and strategic priorities for achieving them

- announced new capabilities
  - CERT Australia
  - Cyber Security Operations Centre (CSOC)
Better coordinate Australia's cyber event response arrangements

Provide a single POC for cyber security information domestically & internationally

Incorporate a number of current activities including GovCERT.au & its services

Complement the Cyber Security Operations Centre (CSOC) within Dept. of Defence
Information Exchanges

- Outcome of the E-Security Review 2008

- Based on forums conducted in the UK and USA

- Currently have three, covering Control Systems, telecommunications & banking & finance
Control System Information Exchange

- A closed forum for the exchange of sensitive technical information between the Australian Government and owners and operators of critical control systems

- Discussion focused on technical threats and vulnerabilities seen within and attributed across industry sectors

- Membership guidelines require participants to undergo a police check

- Information exchanged includes up to Red level under the Traffic Light Protocol
Established as an initiative of the 2009 Defence Whitepaper to provide Australian Government with:

- All-source cyber situational awareness

- Enhanced operational responses to cyber security events of national importance
  - Government and critical private sector systems

- Ability to identify and analyse sophisticated cyber attacks targeting government systems or systems of national interest
Summary

➢ Provide guidance and facilitate information sharing

➢ Increase comprehension of risks and access to effective mitigation strategies

➢ Provide operational support
Cyber Security Strategy

Objectives:
Objective One: All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online

Objective Two: Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers

Objective Three: The Australian Government ensures its information and communications technologies are secure and resilient

Strategic Priorities:
Threat Awareness and Response – improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest

Cultural Change – educate and empower all Australians with the information, confidence and practical tools to protect themselves online

Business-Government Partnerships – partner with business to promote security and resilience in infrastructure, networks, products and services

Government Systems – model best practice in the protection of government ICT systems, including the systems of those transacting with government online

International Engagement – promote a secure, resilient and trusted global electronic operating environment that supports Australia’s national interests

Legal and Law Enforcement – maintain an effective legal framework and enforcement capabilities to target and prosecute cyber crime

Knowledge, Skills and Innovation – promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions