Overview

Western Australia’s (WA) critical infrastructure includes those assets used in delivering the power, water and transport needs that are essential to our social and economic well being. The delivery of these essential services is heavily dependent upon specialised computer systems that control power grids, gas and oil distribution pipelines, water treatment and distribution systems and flood control dams. Some of these systems are large, even by world standards.

Australia’s National Counter-Terrorism Committee (NCTC) has collated a database of Australia’s critical infrastructure and developed guidelines relating to the protection of that infrastructure. These have now been accepted by all the Commonwealth, State and Territory Governments. Collation of the Western Australian database has been undertaken by the Security Planning Coordination Unit (SPCU) of the Department of the Premier and Cabinet on behalf of the State’s NCTC representatives and the State Emergency Management Committee (SEMC). The SPCU is also working with the owners/operators to ensure that security plans, policies and procedures are established.

This examination reviewed progress made by the SPCU and also assessed risk management, IT security management and control system vulnerabilities at three State government agencies.

Key Findings

● The SPCU has completed its preliminary identification and assessment of National and State critical infrastructure assets and is coordinating various security activities. However, the SPCU is being integrated into a new and larger emergency management group incorporating the State Crisis Centre. This is expected by September 2005.

● Control systems have become increasingly vulnerable to cyber attack due to their connection to corporate networks, their improved user friendliness and the increased sophistication of hackers. Risk management is therefore critical. Aspects of the risk management practices at the three agencies are good but some improvements are needed:

   ○ One agency has established a comprehensive risk management framework. The other two agencies are developing such a framework, scheduled for completion by the end of 2005.

   ○ Risk assessments at two agencies have not been prepared for most of their major infrastructure control systems. Accordingly, they have a reduced capacity to manage their security risks.

   ○ The agencies had not ranked cyber threats to critical infrastructure control systems in the high level risk category and need to reassess their security risk models and assumptions.

● Security management practices and system vulnerabilities in the three agencies also need to be addressed:

   ○ Two agencies had a range of vulnerabilities in the remote access arrangements for their control systems.

   ○ One agency had a control system connected to the corporate network without a firewall to isolate it from users on the corporate network. This risks damage to the system by viruses and other forms of malicious code.
One agency had serious and ongoing problems with a key fault management system. This system’s reliability is prerequisite for infrastructure operations.

Responsibilities at two of the agencies for connectivity between the control systems and the corporate systems were not clearly defined. This led to inconsistent application of security policies.

Two agencies did not have schedules for the review of control system firewalls or the maintenance of operating system patches. They also had not undertaken vulnerability assessment and penetration testing of some control systems. This is contrary to accepted good practice as it leaves the extent of vulnerability to hackers and viruses to chance.

**What Should Be Done?**

Agencies should:

- Complete the implementation of their risk management frameworks.
- Identify all their critical infrastructure control systems.
- Ensure that risk management processes cover security threats associated with infrastructure control systems.
- Ensure that risk assessments are completed for the control systems and translated into IT security plans.
- Align and reallocate responsibility for the security of control systems and define roles to ensure that security procedures are carried out effectively.
- Ensure that corporate security policies and procedures cover control systems applications.
- Establish effective processes covering incident response, disaster recovery, physical security, connection of laptops and non-standard devices, virus protection, software updates, firewall management, intrusion detection, vulnerability assessments and penetration testing and monitoring and logging of information.