VICTORIA

Victorian
Auditor-General

Audit summary of Security of Infrastructure Control Systems for Water and Transport

Tabled in Parliament
6 October 2010

Audit summary

Background

Infrastructure critical to the provision of essential water and transport services includes the physical assets, facilities, distribution systems, information technologies and communication networks. This infrastructure relies on control and management systems, such as Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are usually computer-based.

Computer interconnectivity has increased since the 1990s, especially the use of the internet, which has revolutionised the way that the government and broader community communicate and do business. While the benefits of this widespread interconnectivity have been enormous, it also exposes computer systems, and the essential services and critical infrastructure they support, to major security risks.

If not properly controlled, the increased speed and accessibility that benefits intended users can also give unauthorised individuals and organisations access to operational information that is used for mischievous or malicious purposes, including fraud or sabotage.

The Longford gas crisis in 1998 and the electronic attacks on the Maroochy Shire sewerage control system in Queensland in 2000, highlight the need to manage and promote the security and protection of critical infrastructure. If exploited, unauthorised access to infrastructure control systems has the potential to disrupt or disable the provision of essential services. The Australian Security and Intelligence Organisation warns that Australia faces ongoing threats from terrorism, espionage, and foreign interference, including cyber threats.

The ability to keep delivering essential community services depends on a number of factors, including effective computer system security controls and procedures that either prevent unauthorised access or detect and respond to security breaches.

This audit examined the security of infrastructure control systems at selected water and transport operators and oversight of these operators by relevant portfolio agencies.

Conclusions

The risk of unauthorised access to water and transport infrastructure control systems is high. This access could compromise these systems and affect the stable delivery of essential services to the community.

Operators do not have:

- the physical and electronic controls to detect and prevent inappropriate access to their infrastructure control systems
- appropriate governance arrangements, such as risk, emergency and business continuity management, policies and procedures, and monitoring and reporting mechanisms to assure management that their infrastructure control systems are secure.

Operators are not fully aware of the weaknesses in, and risks to their infrastructure control systems.

The responsible oversight agencies, the Department of Sustainability and Environment (DSE), Department of Transport (DOT), and Victoria Police are not fully aware of the weaknesses in infrastructure control systems used by operators for the delivery of essential services. This is because:

- these agencies are not actively monitoring and guiding operators in the management of infrastructure control systems
- there is a lack of clarity among operators about their roles and responsibilities, and those of the oversight agencies, in securing infrastructure control systems.

Findings

Securing infrastructure control systems

Operators are not properly securing their infrastructure control systems. As a result, staff and external parties can inappropriately access and manipulate these systems. Operators recognise this situation, and are developing strategies to address it.

Security processes and controls are not satisfactory and appropriate and do not comply with relevant industry standards, such as:

- Standards Australia AS/NZS ISO/IEC 27001:2005 Information technology, Security techniques—Information security management systems (ISO 27001)
- Standards Australia AS/NZS ISO/IEC 27002:2005 Security techniques—Code of practice for information security management (ISO 27002).

In addition, operators do not have:

- provisions in their contracts with external parties accessing their infrastructure, that address security requirements
- procedures to monitor and control external-party access to infrastructure control systems.

With the exception of one out of the five operators reviewed, security-related design considerations are not incorporated into operators' procurement processes for new infrastructure control systems. Where security requirements are considered by operators, the requirements are determined without reference to an existing security standard.

Operator governance arrangements

While operators have established governance arrangements to help them effectively manage their businesses, there is little evidence that infrastructure control system security issues and details of major security breaches were being discussed with operator boards and senior management for consideration and action. This is not surprising given that most operators do not have a central person or group that takes responsibility for infrastructure control system security.

While all operators had developed risk management frameworks and established many of the framework components, none had effective processes to manage the risks to their infrastructure control systems. None of the operators were fully compliant with the risk management requirements of the *Terrorism (Community Protection) Act 2003.*

In addition, the audit revealed that:

- operators do not have comprehensive up-to-date policies and procedures to manage infrastructure control system security
- information collected and reported to management about security breaches, non-compliance with policies and procedures, information and communication technology (ICT) risks and infrastructure control system vulnerabilities is inadequate
- operators are not adequately monitoring and controlling the infrastructure control systems that external parties manage on their behalf.

Establishing response capabilities

The quality of operators' emergency response and business continuity plans varied. Overall, they do not adequately address issues associated with infrastructure control systems. If a security breach shut these systems down, essential services may be lost for an unacceptable period.

Departmental oversight

DSE and DOT do not:

- actively monitor operator security management of infrastructure control systems
- have mechanisms to assure themselves that security breaches and incidents are reported and acted on
- use suitably qualified and experienced staff to advise operators about securing infrastructure control systems and managing cyber risks
- review and provide feedback on security-related documents, such as risk management, business continuity and emergency response plans. DOT does, however, review operator risk management plans.

Recommendations

Given the sensitive nature of the audit findings, we have provided details of security weaknesses identified and associated recommendations to each operator and the responsible departments, which are not included in this report.

The following generic recommendations apply to all operators of critical infrastructure and providers of essential services, and oversight agencies.

Number	Recommendation	Page
1.	Operators should rigorously review the security of their infrastructure control systems against the relevant state and international security standards and implement improvements, where required.	22
2.	The Department of Sustainability and Environment should: • increase its monitoring of operator ICT and infrastructure control system risk, and business continuity management • use suitably qualified and experienced staff from within the department to provide advice to operators on infrastructure control system security and risk, and business continuity management.	33
3.	The Department of Transport should establish an ICT security team. It should be comprised of suitably qualified and experienced staff to provide advice to operators on infrastructure control system security and risk, and business continuity management.	33

Submissions and comments received

In addition to progressive engagement during the course of the audit, in accordance with section 16(3) of the *Audit Act 1994* a copy of this report, or relevant extracts from the report, was provided to the Department of Transport, the Department of Sustainability and Environment, Victoria Police, and the Department of Premier and Cabinet, with a request for submissions or comments.

Agency views have been considered in reaching our audit conclusions and are represented to the extent relevant and warranted in preparing this report. Their full section 16(3) submissions and comments however, are included in Appendix A.