Security of Infrastructure Control Systems for Water and Transport

Victorian Auditor-General's Report

October 2010

2010-11:15

VICTORIA

Victorian
Auditor-General

Security of Infrastructure Control Systems for Water and Transport

Ordered to be printed

VICTORIAN
GOVERNMENT PRINTER
October 2010

PP No 386, Session 2006–10

Mixed Sources
Product group from well-managed forests and other controlled sources
www.fsc.org Cert no. SGS-COC-004630
© 1996 Forest Stewardship Council
FSC

SYSTEM CERTIFICATION
ISO 14001:2004
SGS

This report has been produced to ISO14001 environmental standards. It is printed on FSC credited Novatech Satin & Media Print Silk paper. The print supplier, Blue Star PRINT has initiated an EMS promoting minimisation of environmental impact thr the deployment of efficient technology, rigorous quality management procedures and a philosophy of reduce, re-use and r

ISBN 978 1 921650 60 4

VAGO

Victorian Auditor-General's Office
Auditing in the Public Interest

The Hon. Robert Smith MLC
President
Legislative Council
Parliament House
Melbourne

The Hon. Jenny Lindell MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my performance report on *Security of Infrastructure Control Systems for Water and Transport.*

Yours faithfully

D D R PEARSON
Auditor-General

6 October 2010

Contents

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.

1 Background

1.1 Introduction

Infrastructure critical to the provision of essential water and transport services includes the physical assets, facilities, distribution systems, information technologies and communication networks.

The infrastructure relies on control and management systems, such as Supervisory Control and Data Acquisition (SCADA) systems. These computer-based systems:

- operate and control power grids, dams, water treatment and distribution facilities, and tram/train power and signalling systems
- collect the data needed to run the businesses and transmit it to central computers that manage and control this data.

Since the early 1990s computer interconnectivity and internet use has revolutionised how the public and private sectors communicate and do business. The speed and access this allows provides obvious benefits, but it also poses major risks to the government's computer systems and to the essential services and critical infrastructures they support.

If not properly controlled, unauthorised individuals and organisations can access or interfere with these operations from remote locations, for mischievous or malicious purposes, including fraud or sabotage.

Events such as 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, the growing number of weaknesses identified have the potential to disrupt or disable the provision of essential services. The Australian Security and Intelligence Organisation warns that Australia will continue to face a persistent threat of terrorism, espionage, and foreign interference, including cyber threats.

The stable delivery of essential services to the community relies on:

- effective operator security controls and procedures to detect and prevent unauthorised access to infrastructure control systems and respond to security breaches
- effective business continuity management and establishing emergency response capability.

1.2 Policy and legislative context

The *Public Administration Act 2004* (PAA) and the *Financial Management Act 1994* (FMA) require public sector agencies to set up good governance arrangements.

Water operators are bound by the *Water Act 1989*, the *Water Industry Act 1994*, and statements of obligations that the Minister for Water issues. Requirements for public and privately owned transport operators are outlined in the *Transport Integration Act 2010* and franchise/lease arrangements, respectively. Under these Acts and arrangements, operators are responsible for the protection and management of essential public services.

Operators of essential services are also subject to the *Terrorism (Community Protection) Act 2003* (the Act) and *Emergency Management Act 1986*. These Acts also state that operators are responsible for protecting and restoring essential services if disrupted.

1.3 Roles and responsibilities

Operators using critical infrastructure for essential water and transport services are primarily responsible for its security, and the security of any associated control systems.

Water sector operators are the state-owned water corporations. Whereas, transport sector operators are private companies that provide transport services to the state government under franchise agreements.

The Department of Sustainability and Environment and Department of Transport oversee the water corporations and transport operators, respectively.

The Department of Premier and Cabinet (DPC) published the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP framework) in April 2007. This framework is based on government and industry partnerships that build a culture of security protection and awareness.

The legislation and CIP framework are designed to build the capability of operators to secure critical infrastructure and the continued provision of essential services in Victoria.

Under the regulatory CIP framework, providers of essential services are primarily responsible for managing security risks associated with service delivery. This includes safeguarding their infrastructure control systems.

The five operators reviewed in this audit operate critical infrastructure and provide essential services, as defined under the Act.

The security and continuity networks structure is at the core of the Victorian critical infrastructure protection management arrangements. Networks include members of state and local governments and owners/operators of critical infrastructure. Together, they consider security, emergency management and business continuity policies and practices for critical infrastructure in Victoria.

Victoria Police's role under the *Terrorism (Community Protection) Act 2003* is to review essential service operators' counter-terrorism exercises. Under the CIP framework, it must also identify and rate the Victorian list of critical infrastructure sites.

1.4 Security standards and good practice

The principles of good governance set out in the PAA, FMA and the whole-of-Victorian-Government (WoVG) policy on information security management include following the international risk and information security standards:

- AS/NZS ISO 31000:2009—Risk management
- ISO/IEC 27001:2006—Information security management systems
- ISO/IEC 27002:2006—Code of practice for information security
- ISO/IEC 27005:2008—Information security risk management.

Other standards relevant to maintaining the security of control systems include:

- WoVG standards updated in 2010:
  - SEC STD 01 Information Security—Management framework
  - SEC STD 02 Information Security—Data classification and management
  - SEC STD 03 Information Security—Penetration testing
  - SEC STD 04 Information Security—Use of portable storage devices
- *Good Practice Guide, Process Control and SCADA Security*, 2006, from United Kingdom's Centre for Protection of National Infrastructure
- *Guide to Industrial Control Systems Security*, 2008, from the National Institute of Standards and Technology, United States Department of Commerce.

1.5 Previous audits

In 2009 the Victorian Auditor-General's Office (VAGO) published *Preparedness to Respond to Terrorist Incidents: Essential Services and Critical Infrastructure* (2008–09:15). It found gaps in the risk management guidelines for owners and operators of essential services and critical infrastructure.

Following this audit, the DPC began reviewing the arrangements for managing risks associated with essential services and critical infrastructure.

In November 2009, VAGO also published a performance audit titled *Maintaining the Integrity and Confidentiality of Personal Information* (2009–10:8), which found that information security risks were not managed effectively.

1.6 Audit objectives and scope

The aim of this audit is to assess whether the systems used to operate, manage and control water and transport infrastructure, are secure.

We assessed:

- the Department of Sustainability and Environment, the Department of Transport and Victoria Police's oversight of the state's critical infrastructure and the associated control systems
- security arrangements of five operators that provide essential services, against a security framework developed from legislative requirements, government policy, industry standards and good practice
- specific security policies, procedures and controls of one of the systems at each operator.

1.7 Audit methodology

The audit was performed in accordance with Australian Auditing and Assurance Standards.

The cost of the audit was $695 000.

1.8 Report structure

The rest of the report is structured as follows:

- Part 2: Operator security
- Part 3: Portfolio agency oversight.

2 Operator security

At a glance

Background

We chose four critical infrastructure operators in the water sector and one in transport, and assessed whether their infrastructure control systems were secure. Operators were assessed against a security framework, based on legislation, government policy, standards, and better practice guidelines. We also examined the use of security controls for selected systems at each operator.

Conclusion

Operator control systems for critical infrastructure are not secure. As a result, the ongoing delivery of essential water and transport services is at risk.

Findings

Operators' security controls do not properly protect infrastructure control systems from unauthorised access.

Operators' security frameworks protecting infrastructure control systems are ineffective because:

- infrastructure control system risks are not properly identified and managed
- information that operators record, monitor and report to management is not enough to effectively oversee security
- policies and procedures are incomplete or outdated
- strategic and business planning processes do not adequately address the management and security of infrastructure control systems
- operators have governance frameworks, but management's oversight of infrastructure control system security is inadequate
- operators do not have the capacity to respond to adverse events impacting on infrastructure control systems.

Recommendation

Operators should rigorously review the security of their infrastructure control systems against the relevant state and international security standards and implement improvements, where required.

2.1 Introduction

We assessed:

- operator security frameworks—generic aspects of security control applicable to all operator systems and operations
- security controls used to protect selected systems at each operator.

The security framework was based on legislative and other requirements, federal and state government policy, relevant standards and industry better practice.

The framework covers:

- securing infrastructure control systems
    - maintaining secure systems
    - securing new systems
    - external-party access
- effective governance arrangements
    - planning and stakeholder engagement
    - management oversight
    - organisational culture
    - risk management
    - policies and procedures
    - information, monitoring and reporting
- establishing response capabilities
    - emergency response
    - business continuity.

2.2 Conclusions

Operator security frameworks are not mature enough to safeguard the infrastructure control systems that operate critical infrastructure. Security controls to protect the systems reviewed are not enough to prevent unauthorised access to operator information and communication technologies (ICT) and infrastructure control systems.

As a result, operators cannot demonstrate that the infrastructure control systems used for the ongoing delivery of essential water and transport services are secure.

2.3 Overall assessment of operator security frameworks

Operator security frameworks were benchmarked against a model that measured the maturity of their security over infrastructure control systems.

The maturity criteria used in the assessment are:

- **Initial**—few of the expected processes and procedures exist
- **Developing**—operator is establishing processes and procedures
- **Established**—effective processes and procedures exist
- **Continuous improvement**—effective processes and procedures exist and are continuously improved.

Figure 2A summarises the results of these assessments for the five operators and their systems.

Figure 2A
Analysis of maturity of infrastructure control system security

Framework elements	Initial (number of operators)	Developing (number of operators)	Established (number of operators)
Securing infrastructure control systems			
Maintaining secure systems	2	3	–
Securing new systems	4	–	1
External-party access	2	3	–
Information and communication technology security governance			
Planning	1	3	1
Stakeholder engagement	1	3	1
Management oversight	4	–	1
Organisational culture	–	4	1
Risk management	–	5	–
Policies and procedures	2	3	–
Information, monitoring and reporting	4	–	1
Establishing response capabilities			
Emergency response	2	2	1
Business continuity	3	2	–

Note: No operators were in the 'continuous improvement' level of maturity.
Source: Victorian Auditor-General's Office.

All operators had some positive processes and procedures. Only one operator used most of the expected elements, but still had some gaps that need attention.

2.4 Securing infrastructure control systems

Historically, control systems for critical infrastructure in the water and transport sectors have been proprietary systems that staff based at the infrastructure facility operated. These were stand-alone systems that did not link to organisational networks or systems.

Modern infrastructure control systems are moving away from these closed networks towards more open systems, linked to corporate and public networks. Applications are using open standards, such as Ethernet, TCP/IP, web technologies and are running on common operating system platforms on servers using UNIX and Windows operating systems.

These changes should reduce operational costs and enhance performance through remote maintenance, control, and update functions. However, this interconnectivity and 'openness' exposes the infrastructure control systems to security weaknesses in any connected corporate networks.

There is more system exposure now due to:

- control systems becoming easier to operate—which means users do not need specialised knowledge
- control systems becoming more complex and interdependent
- an increase in publicly available information about control systems—which means intruder attacks and knowledge of control systems are becoming more sophisticated
- increases in the extent and number of identified weaknesses
- existing security technologies and practices not keeping pace with threats
- increases in remote and wireless connections—creating more opportunities to access systems.

In addition, physical safeguards for these control systems are often inadequate and are vulnerable to structural damage.

The challenge for critical infrastructure operators is to improve efficiency without compromising security. To prevent unauthorised access to their ICT and infrastructure control systems, operators need to maintain secure systems, build security requirements into new and upgraded systems, and manage external-party access to their facilities and systems.

2.4.1 Maintaining secure systems

Based on an assessment of business risk, operators of critical infrastructure should use technical, procedural and management controls to protect the security of their critical infrastructure and associated control systems. System architecture is the conceptual design that defines the structure and/or behaviour of a system.

Operators of critical infrastructure should be able to define their system architecture and apply controls, technologies, and procedures that support the architecture’s objectives.

Security architecture identifies areas that need security controls to preserve the access and integrity of the infrastructure control systems.

We found several deficiencies in the security architecture of some audited operators, mainly around the set up of firewalls, separation of networks, and remote access.

Firewalls

Firewalls, intrusion detection systems and intrusion prevention systems work together to help detect and fight common network attacks, such as service denial, malicious code and spoofing attacks, where a person or program successfully imitates another using false information.

We found that the firewall configuration at one operator could not detect and withstand these common network attacks. There were operators that did not have schedules to review and update their firewall configuration.

Generally, controls are sufficient to detect and prevent modern and evolving threats from malicious software, although infection and anti-virus programs are not always current.

Separation of networks

Attacks can come from internal or external sources. The most basic form of prevention is to separate the infrastructure control systems from internet access and the corporate network. Work on the infrastructure control systems should happen on dedicated computers.

We found some operators had connections between the corporate network and infrastructure control systems, without firewalls to isolate them from corporate users. Without clear definition between infrastructure control systems and corporate systems, security policies and procedures are not consistently applied. There are instances where staff connected to the infrastructure control system from the corporate network to do administrative functions.

Remote access

If it is not properly secured, remote access can provide a ‘back door’ for intruder entry into the network. We found several security weaknesses in operators’ remote access arrangements, including:

- the use of the public telephone networks to access infrastructure control systems
- some remote access software used to administer control system servers had file transfer capability, which allows accidental, or intentional, introduction of viruses or malicious code
- part of the connection between remote field devices and central devices is not secure or encrypted.

In some cases, there was little or no mapping of infrastructure control systems and networks. The appropriate knowledge lies with specific staff members. This is also the case for many procedures governing ICT and control systems.

One of the five operators took a proactive, rather than a compliance-driven approach to the security of infrastructure control systems. This operator's network, system, technical, physical security controls and related administrative processes are generally meeting the security requirements for operating critical infrastructure. However, even this operator could have improved system security by:

- separating infrastructure control systems from its corporate network
- providing better support and improving visibility to senior management.

Conclusion

Operator ICT and infrastructure control systems are not adequately secured. Operators already recognise this situation and are developing strategies to address it.

As a result, staff and external parties can access the control systems that operate infrastructure used to provide essential water and transport services, and it is possible that someone has breached these systems without operators realising.

2.4.2 Securing new systems

In developing new systems, it is important to consider system security requirements. Building security protection measures into new systems is easier, cheaper and more effective than incorporating them into existing systems.

To effectively manage security risks, businesses need to identify milestones during the development of new systems, when security requirements are determined, designed, implemented and confirmed.

We found that operators do not incorporate security considerations when purchasing and developing new infrastructure control systems. When security requirements are considered, they are determined without guidance from an existing security standard.

When developing or acquiring new systems operators focus on operational requirements and capabilities, with only limited regard for security considerations. In most cases it is only after these systems have been in place for some time that security deficiencies are identified and addressed.

As part of the audit, we reviewed a system under development to assess whether operators had built security controls into the system before it went live.

Operators develop and purchase most of their own systems. This system, however, was created by an external developer. The external developer will hand over the new system to the operator when it is finalised.

The operator did a lengthy, detailed and considered functional and non-functional analysis during the design, planning and development phases of the new system. The new system addressed all the components of a modern, robust, resilient and secure technology system.

The system is very different to the current one and will require operational management plans and changes to current system administrative processes. The operator has not prepared plans or processes for the secure operation of the new system.

Conclusion

Operator processes and procedures are not robust enough to assure management that new infrastructure control systems include appropriate security requirements.

2.4.3 Managing external-party access

External parties, such as suppliers, distributors, partners and customers can jeopardise security over infrastructure control systems. Technologies that allow greater interconnectivity between these parties and the operator, such as dial-up access or the internet bring new external threats.

Operators:

- had not identified and assessed the risks associated with external-party access to their critical infrastructure and associated control systems
- generally do not have documented policies and procedures to manage these risks.

Operators were aware of the common procedures and controls used to control the risks associated with external-party access, but they rarely used them.

When operators had outsourced service delivery they also:

- had not built security compliance and reporting requirements into contracts with external parties accessing operator facilities and control systems
- generally did not have processes to update agreements/contracts when there were changes to the security infrastructure, environment and processes
- were not consistently communicating security requirements to external parties
- did not adequately monitor and record external-party access to their systems and the actions of these parties
- are largely unaware of what non-standard, non-vetted plug-in devices, equipment and software are connected to their IT networks by their service providers
- do not receive details of systems changes and regular performance and incident reports from their service providers.

Conclusion

Operators are not adequately addressing the risk of unauthorised access to their infrastructure facilities and ICT systems by external parties.

2.5 Information and communication technology security governance

Sound governance informs effective and consistent approaches to the security of ICT and infrastructure control systems. It also helps to identify gaps and ways to address them. Without consistent governance, attempts to secure these systems can be ad hoc or inadequate.

Effective governance arrangements should use a risk-management approach and include appropriate:

- management oversight
- monitoring and reporting
- policies, procedures and guidelines for security management
- planning
- stakeholder engagement
- security consciousness and awareness.

2.5.1 Risk management

As systems became outdated or were replaced to improve efficiency, operators progressively moved to more open non-proprietary systems linked to their local business and public networks.

With the earlier ‘closed’ systems, there was a low risk of unauthorised access. The move to more open systems has significantly increased the risk for operators. In this environment operators need to be aware of, and manage this risk.

The process for identifying and managing risks, including security risks, is set out in the Australian and New Zealand Standard for Risk Management Standard AS/NZS ISO 31000:2009. Under the *Terrorism (Community Protection) Act 2003* (the Act), a risk management plan must be prepared for all declared essential services, in accordance with the standard.

Once operators identify and rate these risks, strategies must be prepared to mitigate them. Strategies for major risks are included in an organisation-wide risk management plan, while separate risk management plans should be prepared for:

- key operational areas
- each major critical infrastructure asset
- ICT and infrastructure control systems.

These risks to operator systems change over time because of system modifications, outsourcing of operations and environmental and legislative change. Therefore, the risks, and strategies designed to manage these risks, need to be regularly reviewed and updated.

Infrastructure control systems risk management approaches

All operators had developed risk management frameworks for their businesses based on the standard. These frameworks included processes for identifying and assessing operational and strategic risks, and plans that outline the proposed strategies to address unacceptable risks.

All operators had:

- developed detailed risk assessments and mitigation strategies that were recorded in risk management systems
- organisational risk registers that summarised the high-level risks the business faced, and provided brief descriptions of the mitigation strategies.

However, operators were either inadequately addressing, or not addressing, specific ICT and infrastructure control systems risks in the organisation-wide risk registers. There were also no separate risk registers for ICT and infrastructure control systems.

Operators were also using their risk registers as risk management plans. While these registers summarised the high-level risks and had brief outlines of some mitigation strategies, they did not have enough detail to be effective. Information about who was responsible for the mitigation strategies, completion time frames and processes to monitor and update progress against them was not recorded in the registers.

Risk assessment

Our review of the operators' current risk assessments showed:

- none had a complete record or inventory of their infrastructure control systems
- two of the five operators had prepared infrastructure control system risk assessments, which were only prepared in March 2010 and approved by operator boards
- at the other three operators, where infrastructure control system risk was not separately assessed, it was unclear how risk ratings were calculated without risk assessment documents
- risks associated with the operations of external service providers were not identified and assessed.

The two operators that recently assessed risks associated with infrastructure control systems found several previously unrecognised high risks. As this level of risk was not acceptable, operators developed strategies to reduce them. This demonstrates that former risk assessments were either unreliable or out-of-date.

Historically, operators have assessed ICT and infrastructure control system security risks as medium to low. Operators based assessments on likelihood and the possible effects of risks. They generally rated the effect of systems failure as high, but considered the probability of the event to be low. This resulted in a medium- or low-risk rating, and meant operators saw the security risks to their infrastructure control systems as low.

Operators used reported cases of system infrastructure control system breaches to assess the likelihood of unauthorised access. The number of reported cases does not necessarily reflect the total number of breaches. Operators of these systems are reluctant to report breaches because of the negative effect on their reputation.

The control weaknesses we identified indicate that unauthorised access often goes undetected. This means operators do not have a reliable basis for estimating likelihood, and the lack of good-quality information is contributing to the low assessments of risk.

Infrastructure control system security risk mitigation

Our review of operator risk mitigation processes found that:

- the strategies operators developed to reduce high risks to acceptable levels were not in one document and were not detailed enough to assure that risks were effectively managed
- only one of the five operators had an infrastructure control system risk management plan. This plan was prepared in March 2010. When we reviewed the plan there were several 'serious' risks that had not been addressed
- one operator with a lot of outsourced operations did not have a plan to mitigate the risks associated with these services.

Terrorism (Community Protection) Act 2003 requirements

The Act outlines other risk management requirements. It requires providers of essential services to:

- prepare annual risk management plans for these services, in accordance with the Australian and New Zealand Standard for Risk Management Standard AS/NZS ISO 31000:2009
- have these plans audited to make sure they comply with the requirements of the Act
- on request, provide a certificate to the minister confirming compliance with the Act.

Water operators used the *Security Vulnerability Risk Assessment Guidelines* (SVRAG) to identify their critical infrastructure assets. DSE and the water corporations jointly developed SVRAG for the water industry to use to assess whether infrastructure of state significance should be included in the state critical infrastructure register.

The management plans required by the Act have three parts:

- **risk management**—outlines strategies to prevent and detect events that put the operator's business at risk
- **business continuity**—outlines processes and procedures established to restore the operational capability of the business after an event
- **emergency response**—outlines processes and procedures to control the impact of an adverse event and minimise personal and property loss.

The Act includes a definition of a terrorist act as actions that seriously interfere with, disrupt or destroy electronic systems. This includes information systems and systems used to deliver essential services, such as infrastructure control systems.

We found that:

- two of the four operators had prepared terrorism risk management plans for 2009–10. These plans were not finalised until August 2010. They were a good first attempt at addressing the Act's requirements, but lacked information on risk, business continuity and emergency management for ICT and infrastructure control systems. While the other three operators had systems and processes to identify and manage security risks, they did not have plans
- four of the operators used external firms or their internal auditors to review their plans. Auditors employed to assure operators that risk management plans were robust at three of the operators, reviewed their risk management processes but not their plans.

While the wording of the Act makes it difficult to determine what compliant plans look like, none of the plans followed good practice risk management. None adequately addressed the risk management, business continuity and disaster recovery requirements of the Act.

Conclusion

While all operators had developed and started applying risk management frameworks, none of them had effective processes for managing risks to their infrastructure control systems.

None of the operators complied fully with the risk management requirements of the *Terrorism (Community Protection) Act 2003*.

2.5.2 Management oversight

To effectively oversee the security of ICT and infrastructure control systems, operators need:

- to provide governing boards and board committees with reports on ICT and infrastructure control systems and associated risk management issues
- to assign management responsibility for security of ICT and infrastructure control systems to a person or group
- a committee to provide advice and guidance on the security of ICT and infrastructure control systems.

For oversight to be effective, operators need to define, document and communicate the roles and responsibilities of staff, the board and committees involved with securing ICT and infrastructure control systems.

This oversight should assure senior management that the ICT and infrastructure control systems that external parties providing services need to access, are adequately secured.

Board and board committees

All operators have board committees to deal with audit, risk and compliance issues. These committees oversee and report to the board about the security of ICT and infrastructure control systems.

However, operator boards and board committees have limited involvement in ICT and infrastructure control system risk management, high-level systems monitoring, overseeing responses to major incidents and breaches, emergency management and associated policies and procedures.

Senior management support and communication with staff

There was no clear direction and support for the security of ICT and infrastructure control systems from senior management at most operators. Line managers were not regularly conveying security messages to staff to reinforce governance requirements and to encourage them to take security risks seriously.

Roles and responsibilities

Accountability and responsibility for the security of ICT and infrastructure control systems, risk management, development of policies and procedures, emergency management and monitoring and reporting was not always clear. This caused unnecessary double ups or failure to address some functions at all.

The IT group at each operator manages IT security, whereas engineering and operational staff handle security for infrastructure control systems. These groups work together to operate systems and address security issues.

Security management is more consistent and effective if there is a staff member or group that understands both areas of the business. One of the operators reviewed used this approach.

Outsourced services

One operator, which outsourced most of its services to providers, did not regularly communicate with relevant service provider staff on ICT and infrastructure control system issues. This operator relied on the service providers to secure their ICT and infrastructure control systems without assurance.

At this operator, we found that the system security of one of its service providers was sound, but another was not.

Conclusion

All operators have mechanisms for management to oversee their business operations, but with the exception of one operator, there was limited evidence that senior management was overseeing the security of ICT and infrastructure control system.

2.5.3 Monitoring and reporting

Operators of critical infrastructure need information about the following to assist them manage their infrastructure control systems:

- critical infrastructure and its operation
- non-compliance with internal controls and security breaches
- responses to security breaches.

To effectively monitor and report, operators should:

- determine their information needs and set up ways of capturing and reporting on this information
- be able to identify system weaknesses and monitor staff compliance with policies, procedures and internal controls
- have procedures to manage non-compliance.

Information needs

Operators have not decided what information management needs to oversee the security of infrastructure control systems. As a result, the events monitored and information reported to management was inadequate.

Two operators did not have software that could detect external, unauthorised access to their business and control system networks or processes to record this access.

Four of the operators did not systematically log and monitor:

- user or email/web traffic activity
- trends within local and external networks
- site and dial-up access, downloads, and bandwidth usage.

We expected operators to have systems that report on malicious software activity, failed user login attempts, unauthorised changes and infrastructure control system security incidents.

We found little evidence that operators were conducting audits to identify unacceptable software use, inappropriate connection of devices to the systems, and physical and logical security around infrastructure control systems, including field devices. There was also scope for greater internal audit involvement in assessing system security.

Systems vulnerability and monitoring compliance

One of the operators reviewed did several vulnerability assessments over a number of years. These identified serious security risks. In response, the operator created several major internal projects to address the identified weaknesses.

In other operators, vulnerability and penetration testing was very limited. Operators did not have programs or plans to regularly carry out vulnerability or penetration testing.

Only one operator took advantage of the Federal Attorney-Generals Department’s initiative that pays for half the cost of the penetration testing.

Most of the operators had staff exit procedures and a checklist that included reviewing and cancelling user access. However, these processes were not operationally active and did not include adjustments to user privileges for promotions, transfers, or when responsibilities changed.

There was poor communication between one operator and its service providers about the security of its infrastructure control systems.

Managing non-compliance

Security policies, procedures and internal controls are only effective if operators have ways of monitoring staff compliance and managing non-compliance. We found that monitoring and follow-up of staff compliance with policies, procedures and internal controls were generally inadequate.

Conclusion

The current level of information captured, monitored and reported to executive management is not enough to assure them about the security of their ICT and infrastructure control systems. As a result, they are likely to be unaware of unauthorised employee and external-party access to sensitive systems and information.

2.5.4 Security policies and procedures

To help staff perform their roles, it is important to have operational rules that outline how the business will address potential risks. These rules should reflect legislative requirements, national and international agreements, government policy decisions, operator policies and internal requirements. Operators should outline all these requirements in a policy and procedure manual, along with guidance about how to apply them.

Where policies are management and control system-specific, they should specify the devices covered by the policy, indicate the protocols and applications than can run on the network, who has access, and from where, and the operations that users (or a function) can perform.

Operators need to be assured that effective and comprehensive policies exist for the ICT and infrastructure control systems they run, and for the systems their service providers manage.

The audit found that none of the operators had comprehensive policies and procedures on securing their ICT and infrastructure control systems. Where ICT policies and procedures exist they:

- were often out-of-date
- did not have user manuals, configuration manuals and technical documentation or other procedures or guidelines to support them
- were generic, with no business unit specific, site specific or technology (platform/device/system) specific policies and procedures.

Conclusion

Operators did not have complete, up-to-date policies and procedures on the security of ICT and infrastructure control systems.

Where relevant policies and procedures existed they had limited scope, currency and applicability. It was clear that the use of consistent practices and procedures depends on staff knowledge and awareness of ICT security risks.

2.5.5 Planning

Operators with sound security arrangements address issues relating to infrastructure control systems through their strategic and business planning processes.

There should also be separate strategic plans for the corporation's ICT and infrastructure control systems that address system security issues. In a mature ICT environment, operators would base planning on recognised standards, such as ISO/IEC 27001:2006, 27002:2006 or 27005:2008.

We found:

- there is little or no mention of ICT and infrastructure control systems in operator strategic and business plans
- only two of the five operators had up-to-date ICT plans that deal with the corporate information systems and applications
- none of the operators had strategic plans for their infrastructure control systems.

2.5.6 Stakeholder engagement

Operators should identify and actively engage with relevant stakeholders. External stakeholders include other operators of critical infrastructure, customers, regulators, professional bodies and industry associations. Internal stakeholders include operational units relying on these systems and the data they generate, ICT users, staff managing and maintaining ICT, project managers, application and systems developers, operational managers, the board of management, project steering groups, staff involved in developing and establishing new systems and operators of infrastructure control systems.

Operator engagement with stakeholders with an interest in securing ICT and infrastructure control systems was inconsistent. This has been due to factors, such as:

- security and continuity networks not adequately considering infrastructure control system security issues
- operators not having stakeholder management plans for ICT and infrastructure control systems. Some operators did not have any stakeholder management plans
- operators not having strategies and processes for involving stakeholders in securing ICT and infrastructure control systems.

Conclusion

Overall, operators' strategic and business planning processes do not adequately address the management and security of ICT and infrastructure control systems.

Relevant stakeholders are not having enough input into the management and security of ICT and infrastructure control systems.

2.5.7 Security consciousness and awareness

Employees are both the most important control and the biggest threat to security, with the success of any technical or procedural security protection measure ultimately relying on staff actions.

They have a critical role in applying security controls and in alerting management to non-compliance and breaches. As a result, they need to be aware of the security risks facing the corporation and their responsibility in:

- complying with its policies and procedures
- reporting non-compliance with policies and procedures and system breaches.

When there was no connection between infrastructure control systems, corporate networks and the internet, operational areas managing infrastructure control systems and ICT staff did not need to be aware of each other's roles and responsibilities. Once these systems were connected, this awareness was necessary to secure these systems. This awareness happens through the provision of general awareness and education programs and staff training.

Security awareness helps reduce human error and misuse of operator assets. Awareness programs are critical to fostering a strong system security culture.

We found that operator staff had a basic awareness of security issues and the appropriate responses to them. However, staff:

- involved in operating infrastructure control systems were often unaware of IT security requirements and IT security staff are often unaware of security arrangements around infrastructure control systems and their operating environment
- do not consistently apply operator security policies and procedures
- do not, as a matter of course, identify and report non-compliance with security policies and procedures.

This situation is the likely result of operators' limited security awareness and education programs, which did not include courses dealing with security issues in their staff training programs.

We also found little evidence of operators developing broader strategies to educate and raise staff awareness around security issues.

Conclusion

Operators and their staff do not have enough awareness of the advanced and evolving threats to infrastructure control systems. Compounding this lack of awareness is the absence of effective security education programs.

2.6 Establishing response capabilities

External events that affect the operation of critical infrastructure can cause major property damage, public inconvenience, disruptions to essential services delivery and affect community wellbeing.

Appropriate response capabilities minimise any immediate impacts, and help operators recover quickly from service disruptions.

Operators reflect their ability to respond appropriately in incident management, disaster recovery and business continuity plans. Collectively, these plans show which operations it could re-establish after adverse events, and under what circumstances.

An operator with an appropriate response capability should:

- integrate its risk management and business continuity management
- choose a team to respond to suspected security incidents
- have an early warning system that notifies appropriate personnel of security alerts and incidents
- create processes and procedures to monitor, assess and initiate responses to security alerts and incidents. Possible responses may include more vigilance, isolating systems, applying patches, or mobilising security response teams
- have formal reporting and review of security incidents involving critical infrastructure and associated control systems
- have appropriate electronic security response procedures
- have disaster recovery plans for critical infrastructure and associated control systems and business continuity plans for the essential services provided
- maintain and regularly test disaster recovery and business continuity plans.

In 2004, the Department of Premier and Cabinet State Coordination and Management Council asked government agencies to prepare business continuity plans by 30 September 2004. Based on the *Australian/New Zealand Standards Handbook of Business Continuity Management* (HB 221:2003), the plans were coordinated via the Central Government Response Committee (CGRC), which the Department of Premier and Cabinet supports.

In 2006, CGRC approved the Victorian Government Escalation Protocol, requiring all agencies to escalate their security plans if the threat environment changes.

Emergency response

All operators adopted the emergency management framework from the emergency management manual and had emergency response plans, and early warning and response procedures. However, these plans and procedures were not comprehensive, up-to-date, and were largely untested.

Operators also had response plans for their annual counter-terrorism exercises. Mostly these exercises did not include responses to attacks on ICT and infrastructure control systems.

Business continuity

All operators have principle-based documents that deal with how they will re-establish their businesses after an adverse event. However, their ICT recovery strategies and procedures:

- do not adequately cover the effective and efficient recovery of ICT and infrastructure control systems
- are often not documented
- have not been properly tested.

Two of the operators' business continuity plans were not up-to-date and so did not reflect changes in the operating environment. There was no integration between these plans and their risk management processes.

If operators' followed their plans, most would not be comprehensive or robust enough to minimise business disruption to acceptable levels.

Conclusion

Operators do not have appropriate response capabilities to respond to a major ICT incident, minimise its impact, reinstate ICT and infrastructure control systems and restore business operations in an acceptable time frame.

Recommendation

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.

3 Portfolio agency oversight

At a glance

Background

The Department of Sustainability and Environment and the Department of Transport have oversight responsibility for water and transport operators respectively. Victoria Police reviews essential service operators' counter-terrorism exercises, as well as identifying and rating critical infrastructure sites.

Conclusion

Portfolio agencies have not effectively monitored and supported operators to manage their infrastructure control systems risks. As a result, the emerging information and communication technology (ICT) risks and vulnerabilities facing the state's essential services have not been identified and prioritised for attention.

Findings

- Oversight agencies' monitoring and review does not identify ICT and infrastructure control system security issues in water and transport operators.
- Portfolio agencies have not used suitably qualified and experienced staff to advise operators about securing infrastructure control systems and managing cyber risks.
- The terrorism protection framework in the *Terrorism (Community Protection) Act 2003* and the Department of Premier and Cabinet's critical infrastructure protection framework are not fully implemented. Accordingly, infrastructure control systems are not sufficiently secured.

Recommendations

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.

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.

3.1 Introduction

To secure the state’s infrastructure control systems, oversight of the operator’s management of these systems must be effective. The Department of Sustainability and Environment (DSE) oversees water operators, the Department of Transport (DOT) oversees transport operators and Victoria Police oversees the counter-terrorism exercises and the development of critical infrastructure lists for all operators.

The legislation and guidance that directly impacts on the security of these systems includes the:

- *Terrorism (Community Protection) Act 2003* (the Act)
- Department of Premier and Cabinet’s *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP framework) 2007.

3.1.1 *Terrorism (Community Protection) Act 2003*

Under the Act, providers of declared essential services are responsible for preparing risk management plans for the declared essential services they provide. The Act makes it clear that the risks that need to be addressed include both physical risks and risks to electronic systems, such as information, communication and control systems.

Under the Act, Victoria Police must supervise and consult the relevant department about the format and timing of testing exercises for operators’ risk management plans. The relevant minister must supervise all counter-terrorism exercises under Part 6 of this Act. The Chief Commissioner must provide a written report to the relevant minister about the adequacy of the exercises.

Apart from representing the relevant ministers in the annual training exercise, the Act does not specify a particular role or responsibility for DSE or DOT.

3.1.2 *Victorian Framework for Critical Infrastructure Protection from Terrorism*

The arrangements in the Act are supported by the CIP framework, which includes guidance and coordination arrangements for government and industry’s joint strategies for protecting Victoria’s critical infrastructure.

Risk management is the main tool used to respond to the threat of terrorism.

Operators of critical infrastructure are responsible for security management. The roles and responsibilities of DSE, DOT and Victoria Police under the CIP framework are outlined below.

Department of Sustainability and Environment

DSE’s role is to:

- provide leadership on protection of critical water/sewerage infrastructure
- act as the control agency during water/sewerage-related incidents and dam safety emergencies
- make sure water authorities comply with policy and regulatory requirements, particularly in emergency management and protection of critical infrastructure
- communicate information that is not time sensitive to owners/operators
- participate in, and support, the national critical infrastructure protection arrangements through the Water Industry Advisory Group
- chair the Water Security and Continuity Network (SCN).

SCNs include representatives from state and local governments and the owners/operators of critical infrastructure. Together, they consider security, emergency management and business continuity policies and practices for specific critical infrastructure sectors in Victoria.

Department of Transport

DOT’s role is to:

- make sure security risk and emergency management is adequate within portfolio critical infrastructure sectors—public transport, road and rail system, ports and marine environment, and freight
- provide strategic advice to government and coordinate critical infrastructure sectors so it is capable and prepared to respond to emergencies, as well as supporting national critical infrastructure protection arrangements
- communicate information that is not time sensitive to owners/operators
- participate in, and support, the national critical infrastructure protection arrangements through the three Transport Information Assurance Advisory Groups (IAAG)—aviation, rail and maritime—and the Communications IAAG
- co-chair the Transport SCN.

Victoria Police

The role of Victoria Police is to:

- identify Victoria’s critical infrastructure
- provide protective security advice and develop protective security strategies to counter terrorism
- tell owners/operators of critical infrastructure about relevant threat information
- make sure there are arrangements to protect essential government services, such as utilities and key facilities
- develop and communicate with owners/operators of critical infrastructure the agreed type of response expected for each level of threat and alert
- help owners/operators of critical infrastructure develop, validate and audit risk management plans
- establish and maintain communication with owners/operators
- gather and communicate information to relevant agencies
- conduct and participate in exercises.

DPC have almost completed a review of the CIP framework. Discussions with the department indicate that the proposed changes to the CIP framework will:

- clarify the roles and responsibilities of the operators and portfolio agencies
- provide guidance material to help operators meet their obligations under the Act.

3.2 Conclusions

While the oversight arrangements outlined in the Act and the CIP framework are the same for all operators, the level of monitoring, guidance and support provided by DSE and DOT varies.

Based on the findings of our audit of operators, which show their infrastructure control systems are not secure, the portfolio agencies have not effectively monitored and supported operators to manage the risks to these systems.

The government's terrorism protection framework is not effective in securing infrastructure control systems because operators and oversight agencies do not fully comply with the requirements of the CIP framework.

3.3 Portfolio department oversight

3.3.1 Monitoring and reporting

Operators need to show oversight agencies that they are properly monitoring their performance. This would assure agencies that they are effectively managing non-compliance with government and departmental security requirements and are continuously improving their security procedures.

To be totally effective this would require operators to:

- gather information about systems security management activities
- monitor operator compliance with government/department security requirements and identify security breaches
- monitor operator progress in delivering security management strategies
- assess operator performance against key performance indicators
- identify responses to non-compliance and security breaches.

They should regularly report this information to departments.

The Department of Sustainability and Environment

DSE's Water Industry Division (WID) has collected strategic risk information from water corporations and developed an overall risk profile that includes ICT risks. WID has developed and implemented several frameworks and processes to promote, monitor and test continuous improvement in the governance and risk management of the water sector. The State Emergency Mitigation Committee has done a number of emergency risk assessments for the state and found 18 emergency risks and residual risk curves, including ICT risk that make up Victoria's emergency risk profile.

Before our audit, DSE had not ranked the risks to operator-managed ICT and infrastructure control systems as major. As a result, it was not closely monitoring these risks.

In light of our findings, which showed weaknesses in operator security over ICT and infrastructure control systems, DSE needs to review its level of operator monitoring.

Operator compliance

DSE does not directly monitor operator compliance with security requirements. It relies on the assurance from operator audits under the Act and annual training exercises. This assurance comes through the operator’s internal audit or through an external organisation.

The level of audit assurance includes:

- having a risk management plan that is compliant with the Act
- having an emergency management plan for its annual counter-terrorism exercise that complies with the Act
- being able to produce a risk management plan, in compliance with the Act.

A recent audit report provided to DSE showed that the operator was not complying with the Act.

Essential Services Commission audits

The Essential Services Commission (ESC) conducts audits on a set of performance indicators that operators must report on annually. These audits deal with issues, such as water treatment, customer service and response times for burst mains, but do not address security issues. In the past, audits covering risk management and emergency management stated in the statement of obligations have been included in the ESC audit process, based on the audit scope that the Minister for Water sets.

The Department of Transport

DOT meets with operators to discuss computer system issues as part of the franchise agreement. However, there are no procedures for monitoring and reporting to the department on the security of infrastructure control systems. DOT is planning to create an assurance program to do this as part of its review of information security management. Threat and risk assessments of operator systems are also planned as part of this review.

DOT supervises exercises that the transport sector runs for essential services, under the requirements of the Act.

Internal audit does not have an active role in the security and management of infrastructure control systems for rail transport.

3.3.2 Relationship management

The effectiveness of portfolio departments' oversight is largely dependent on the relationship they have with operators.

The Department of Sustainability and Environment

Operators deal with the DSE's WID on issues affecting the industry. This engagement is through:

- defining the roles and responsibilities of the parties
- regular meetings
- IAAG meeting attendance
- regular one-on-one contact
- workshops on relevant issues
- direct contact to resolve specific issues.

WID collects strategic risk information, develops risk profiles and helps operators develop and test good governance practices.

Overall, DSE has a good working relationship with operators. However, the operators are not always clear on their roles and responsibilities. For example, operators were misguided in their belief that the department reviewed and approved their risk management plans. Under the Act, the operators are responsible for preparing risk management plans in accordance with the Act. They are also required to have them audited annually. The Act does not require DSE to approve these plans.

There was also confusion about the meaning of critical infrastructure. The CIP framework defines critical infrastructure as:

> '… those physical facilities, supply chains, information technologies and communication networks which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of Victoria and its community.'

Significant is defined as:

> 'An event or incident that puts at risk public safety and confidence, threatens our economic security, harms Victoria's competitiveness, or impedes the continuity of government and its services.'

The CIP framework categorises critical infrastructure into four categories—vital, major, significant and low. Two water operators did not believe any of their infrastructure was critical because none of it was classified as vital. As a result, they do not think the CIP framework applies to them.

The Department of Transport

DOT worked closely with the operator's technology group during the transition to the new franchise arrangement.

There are many forums and informal meetings where DOT and the operator discuss and resolve issues, including:

- meeting with the rail operator as required under the franchise agreement
- meeting with the operator's technology group fortnightly to exchange views and ideas about technology and systems.

Although the operator and DOT are still clarifying their roles and responsibilities, they have a good working relationship.

3.3.3 Guidance and support

Oversight agencies can help operators secure their infrastructure control systems through:

- policies and procedures
- training programs, working groups and presentations
- specific advice and guidance to agencies.

Policies and procedures

It is important for the government to set up rules to help operators secure infrastructure control systems and comply with legislative requirements, national and international agreements, government policy decisions and ministerial directives.

The government should also create compliance procedures and guidelines. These should cover governance, risk management, asset security, incident response, disaster recovery, compliance requirements and consequences for non-compliance.

Training programs, working groups and presentations

Training programs, working groups and presentations:

- help operators understand the threats and implications of risks to infrastructure control systems
- make operators aware of government and departmental requirements
- build skills to help operators protect their assets.

Provision of specific advice and guidance to agencies

From time to time, operators will need advice and guidance on dealing with specific issues. Oversight agencies need procedures to help operators resolve these problems.

The Department of Sustainability and Environment

Given DSE's oversight model is largely based on self-regulation, it prepares limited procedures and guidelines for the industry. Infrastructure security is dealt with under the Office of Water emergency response protocols:

- Water and Sewerage Infrastructure Emergencies—Emergency Response Notification Protocol between DSE and Victorian Water Corporations
- Managing Threats Against the Water Supply and Sewerage System.

These protocols deal with notifying relevant parties in an emergency, and the procedures metropolitan operators must follow if they receive a threat from an external party.

DSE provides security guidance and advice to operators through:

- inviting expert speakers to speak at SCN meetings
- running occasional workshops and seminars on topics, such as fire preparedness
- providing operators with access to the latest information on security matters through the Commonwealth's Water Services IAAG forums
- provision of the water infrastructure *Security Vulnerability Risk Assessment Guidelines*
- organising Australian Security Intelligence Organisation briefings
- providing training opportunities/programs run by the Commonwealth's Attorney-General's Office and others
- offering access to Australasian Inter-service Incident Management System training.

DSE also gathers operator information for statewide water and sewerage risk profiles, which it provides to the industry. It organises operator meetings where feedback on the results of their emergency exercises is shared.

Feedback and advice is given to operators on request. This advice covers a wide range of topics, including risk assessments and emergency management.

Our audit of water operators identified problems with infrastructure control systems security, and risk and emergency management. We believe that more DSE guidance and support would have assisted operators manage the security of their infrastructure control systems better.

DSE's lack of guidance and support resulted from it:

- assessing the risks to these infrastructure control systems as medium to low
- not having suitably qualified and experienced staff to advise operators on ICT, risk prevention and detection strategies, security of infrastructure control systems and cyber risks.

Other departments, including DOT and the Department of Primary Industries, have recognised the need to provide specialist advice to the private and public agencies they oversee. They are setting up specialist teams to help their staff meet these challenges.

The Department of Transport

There is a contractual requirement in the franchise agreement for the operator to:

- get permission from DOT before operational control systems are changed
- maintain a level of technology currency.

DOT does not have any policies or procedures relevant for infrastructure control system security. It is reviewing its information security management and governance arrangements. Infrastructure control system security policies and procedures will be addressed as part of this process.

Assurance processes will be included in the overall information security management, which will show whether operators are complying with these policies and procedures.

DOT does not provide any training or development activities to operators around infrastructure control systems.

DOT supports operators in developing their terrorism risk management plans and developing counter-terrorism exercises. It has developed the risk management kit for terrorism, which includes a guide on planning and conducting exercises; however, it has not produced any guidance material for operators about the security and management of infrastructure control systems.

Advice and/or guidance about the security and management of infrastructure control systems are provided in franchisee/department forums.

In recognition of the security risks facing ICT and infrastructure control systems that transport operators manage, DOT wants to help by identifying and managing these risks and providing specialist ICT expertise.

3.3.4 Taking corrective action

For operators to keep improving infrastructure control systems security, oversight agencies need to effectively address non-compliance with government requirements, security breaches and identified system weaknesses or vulnerabilities as soon as they arise.

The Department of Sustainability and Environment

Water operators did not report any major non-compliance issues or security breaches to DSE in the past three years. DSE has powers to get operators to address any breaches, where appropriate.

As the ‘control agency’ for water-related incidents, DSE can escalate an incident so that the State Control Centre is activated.

DSE has played the role of advisor, observer and support agency in state and federal level emergency exercises, such as:

- Exercise Isabelle—National Mutual Aid exercise—December 2009
- annual terrorism exercises
- Cyber Storm 3—International cyber terrorism exercise—September 2010.

The Department of Transport

Transport operators did not report any major non-compliance issues or security breaches to DOT by in the past three years.

DOT’s Security and Emergency Management Division (SEMD):

- coordinates the transport sector’s involvement in multi-agency emergency management exercises and acts as a conduit between the transport sector and the government emergency management structures
- manages an emergency coordination facility that includes an incident room equipped to process information, prepare situation reports and coordinate functions across the department.

The division does not provide specialist advice on ICT or infrastructure control system security.

DOT takes direct responsibility for the acquisition and development of new systems, including making sure these systems are properly secured before being they go live.

Before 2009, DOT largely relied on operators to establish and maintain secure infrastructure control systems. In November 2009, VAGA tabled *Maintaining the Security and Confidentiality of Personal Information*. This audit report found weaknesses in government agencies’ handling of personal information, particularly the ineffective management of information security risks.

Following our report, DOT began reviewing its information management practices and associated security. An information security management and governance structure that includes appropriate expertise in ICT security is part of DOT’s new approach to information security management. Information security resources will support staff in this area and become increasingly involved in ICT and infrastructure control system security, along with transport operators. We were advised that this team will also liaise with SEMD to make sure information security management is properly addressed under the Act and the CIP framework.

3.3.5 Conclusion

DSE has a needs-based approach to oversight. It acts as a conduit for third-party advice and guidance, helps water corporations work together, collects information on risk and communicates it to the industry, and addresses problems as they arise. DSE considers it does not have a role setting specific policies and procedures, or directly monitoring compliance with statutory or other obligations.

DOT has used a more active approach to reviewing and providing advice on risk and emergency management and the terrorist risk management plans that transport operators develop, but also provides a limited oversight role.

The audit of the operators showed that they did not have mature security frameworks and security controls that can adequately secure their infrastructure control systems. Neither DSE, nor DOT was aware of the risks to these systems.

Recommendations

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.

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.

3.4 Victoria Police oversight

Under Part 6 of the Act, it is Victoria Police's responsibility to supervise and consult relevant departments about the timing and format of exercises to test risk management plans of operators.

Under the CIP framework, Victoria Police has been given extra responsibilities, including:

- making sure there are arrangements to protect essential government services, such as utilities and key facilities
- developing and communicating with owners/operators of critical infrastructure about the agreed response for each level of threat and alert
- helping owners/operators of critical infrastructure in their development, validation and audit of risk management plans.

To properly perform this role, Victoria Police needs a good understanding of operator businesses, risk management, and ICT and infrastructure control system security. Victoria Police acknowledges that it does not have this knowledge and capability and believes that relevant government departments are responsible for the broader oversight of operators.

Victoria Police believes that the threat of a terrorist-based attack on ICT infrastructure control systems does not warrant its specific attention. Priority is given to terrorist threats with a higher likelihood.

The following Victoria Police oversight activities were examined:

- reviewing operator counter-terrorism exercises
- advice and guidance
- taking corrective action.

3.4.1 Reviewing operator counter-terrorism exercises

Victoria Police reviews the effectiveness of counter-terrorism exercises and reports to the relevant minister on their adequacy. More than 40 emergency exercises were assessed in the past year.

These reviews:

- assess the effectiveness of the operational parts of the security, risk and emergency management plans
- use lessons from these exercises to help operators improve their business service continuity.

To date, several exercises have been assessed and reported as inadequate. When this happens, Victoria Police works with the relevant department to help the operator meet the expected standard.

Victoria Police has not defined what an ‘adequate exercise’ is and is in discussions with government to determine its meaning.

3.4.2 Advice and guidance

Sometimes operators need advice and guidance about dealing with specific issues. Victoria Police provides general guidance on physical security to operators of critical infrastructure and essential services. It provides most of this guidance through its participation in forums, such as:

- **Security and Continuity Networks**—conducted every three to six months, or as required
- **Security and Continuity Network Coordinating Group**—Victoria Police co-chairs the group with the Department of Premier and Cabinet
- **Sectorial Threat Assessments**—happen roughly every two years, or as required. These are facilitated by the Commonwealth Attorney-General’s Department in partnership with Victoria Police
- **Infrastructure Assurance Advisory Groups**—national level meetings with government and industry operators conducted biannually
- **annual all-sector forums**.

Operators can also approach Victoria Police for specific advice. The advice can be given verbally or in writing, depending on the sensitivity of the information, and can take many different forms, including:

- a letter, acknowledging the unit's visit and highlighting any obvious security gaps identified
- a rapid risk assessment, which may be a formal short report outlining physical security issues, along with photographic evidence
- a full security risk assessment that may take days and includes a comprehensive, multi-page security report
- feedback on counter-terrorism exercises
- intelligence from local, national and overseas sources, and information from national threat assessments.

3.4.3 Site evaluations

Victoria Police provides physical security assessment and advice to site operators on the critical infrastructure list, and to providers of declared essential services. There were about 150 site visits/evaluations in the past year. This advice does not extend to security over ICT and infrastructure control systems.

Officers in charge of police stations also have a program to visit critical sites in their local service area to assess physical security.

3.4.4 Taking corrective action

When Victoria Police believes the operator has not run an adequate counter-terrorism exercise, it asks for input from the relevant government department and operator to assess areas needing further development. It runs workshops or further developmental exercises to improve the standard. There is no requirement for operators to comply with Victoria Police's recommendations from the security risk assessments.

It offers workshops and specific advice to the operator. The Critical Infrastructure Protection Unit liaises with police from the local service area and coordinates the investigative or operational response to actual or potential threats of security breaches.

3.4.5 Conclusion

Victoria Police has given operators useful advice about critical infrastructure physical security. While Victoria Police is aware of emerging threats in this area, it does not have the expertise in electronic systems, cyber risks and threats to the security of ICT and infrastructure control systems to help and advise operators to secure these systems.

Appendix A.
Audit Act 1994 section 16—submissions and comments

Introduction

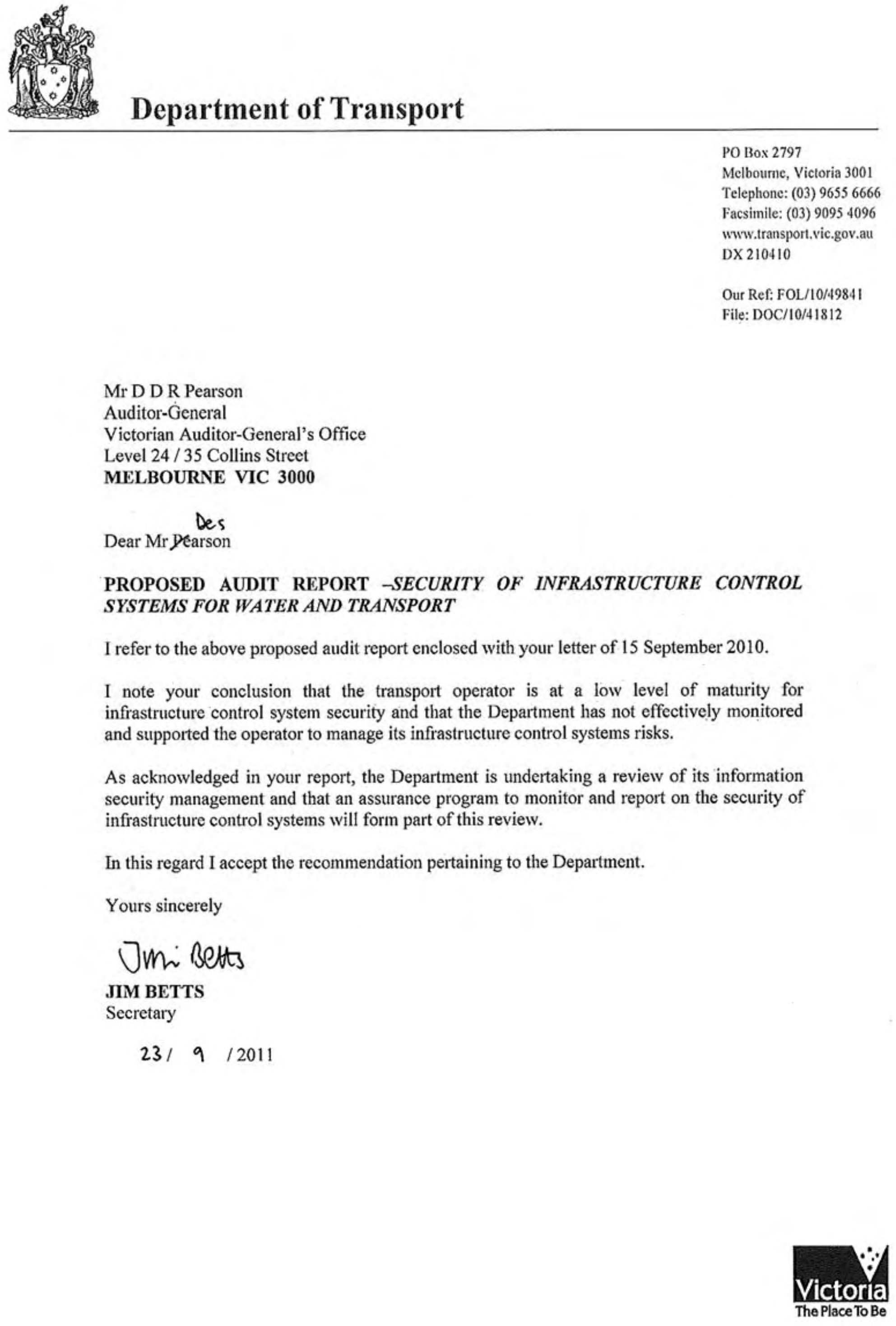
In accordance with section 16(3) of the *Audit Act 1994* a copy of this report was provided to the Department of Transport, the Department of Sustainability and Environment, Victoria Police and the Department of Premier and Cabinet with a request for submissions or comments.

Responses were received as follows:

The submissions and comments provided are not subject to audit nor the evidentiary standards required to reach an audit conclusion. Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Submissions and comments received

RESPONSE provided by the Secretary, Department of Transport



Department of Transport

PO Box 2797
Melbourne, Victoria 3001
Telephone: (03) 9655 6666
Facsimile: (03) 9095 4096
www.transport.vic.gov.au
DX 210410

Our Ref: FOL/10/49841
File: DOC/10/41812

Mr D D R Pearson
Auditor-General
Victorian Auditor-General's Office
Level 24 / 35 Collins Street
MELBOURNE VIC 3000

Dear Mr ~~Pearson~~ Des

PROPOSED AUDIT REPORT –*SECURITY OF INFRASTRUCTURE CONTROL SYSTEMS FOR WATER AND TRANSPORT*

I refer to the above proposed audit report enclosed with your letter of 15 September 2010.

I note your conclusion that the transport operator is at a low level of maturity for infrastructure control system security and that the Department has not effectively monitored and supported the operator to manage its infrastructure control systems risks.

As acknowledged in your report, the Department is undertaking a review of its information security management and that an assurance program to monitor and report on the security of infrastructure control systems will form part of this review.

In this regard I accept the recommendation pertaining to the Department.

Yours sincerely

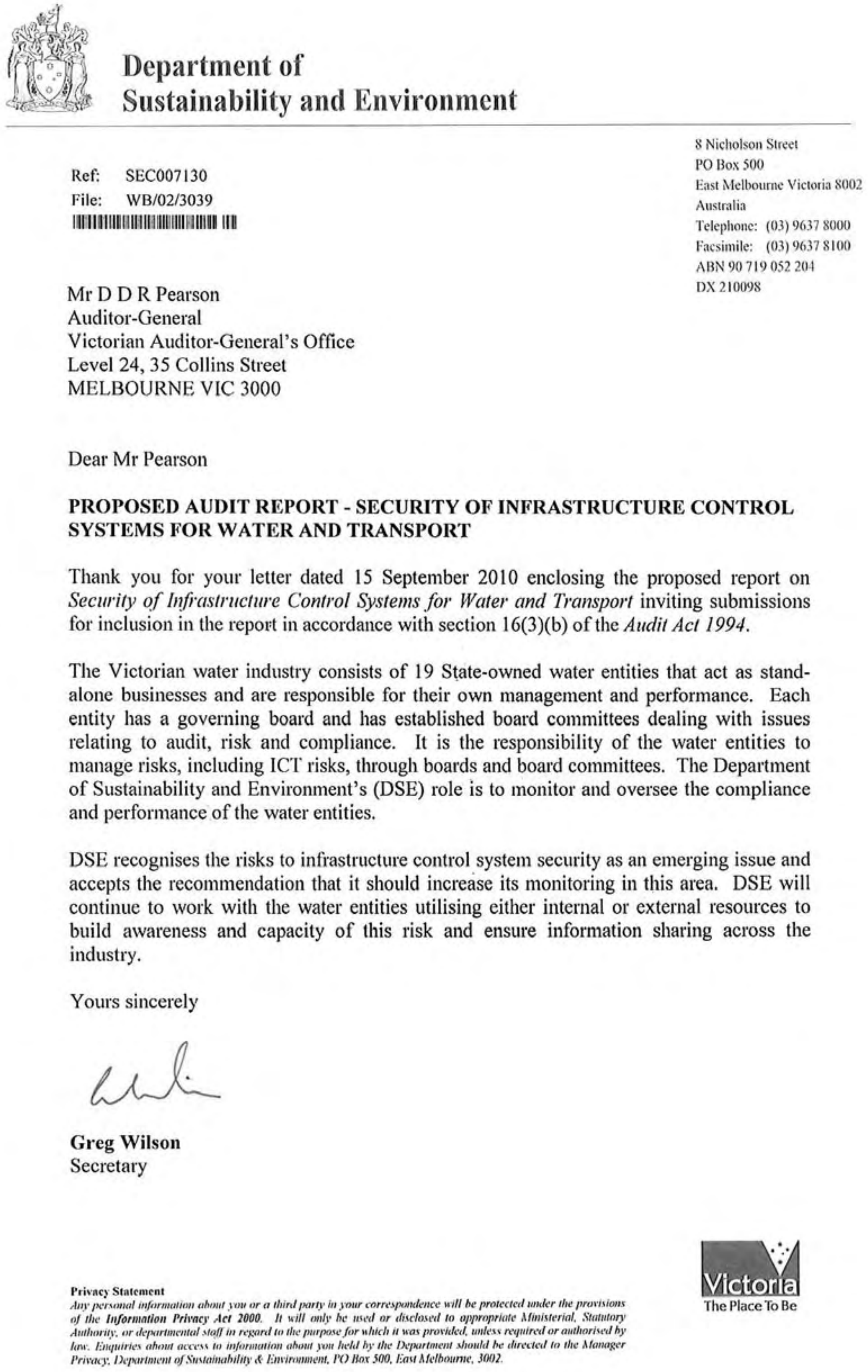
Jim Betts

JIM BETTS
Secretary

23/ 9 /2011

Victoria
The Place To Be

RESPONSE provided by the Secretary, the Department of Sustainability and Environment



Department of
Sustainability and Environment

8 Nicholson Street
PO Box 500
East Melbourne Victoria 8002
Australia
Telephone: (03) 9637 8000
Facsimile: (03) 9637 8100
ABN 90 719 052 204
DX 210098

Ref: SEC007130
File: WB/02/3039

Mr D D R Pearson
Auditor-General
Victorian Auditor-General's Office
Level 24, 35 Collins Street
MELBOURNE VIC 3000

Dear Mr Pearson

PROPOSED AUDIT REPORT - SECURITY OF INFRASTRUCTURE CONTROL SYSTEMS FOR WATER AND TRANSPORT

Thank you for your letter dated 15 September 2010 enclosing the proposed report on *Security of Infrastructure Control Systems for Water and Transport* inviting submissions for inclusion in the report in accordance with section 16(3)(b) of the *Audit Act 1994*.

The Victorian water industry consists of 19 State-owned water entities that act as stand-alone businesses and are responsible for their own management and performance. Each entity has a governing board and has established board committees dealing with issues relating to audit, risk and compliance. It is the responsibility of the water entities to manage risks, including ICT risks, through boards and board committees. The Department of Sustainability and Environment's (DSE) role is to monitor and oversee the compliance and performance of the water entities.

DSE recognises the risks to infrastructure control system security as an emerging issue and accepts the recommendation that it should increase its monitoring in this area. DSE will continue to work with the water entities utilising either internal or external resources to build awareness and capacity of this risk and ensure information sharing across the industry.

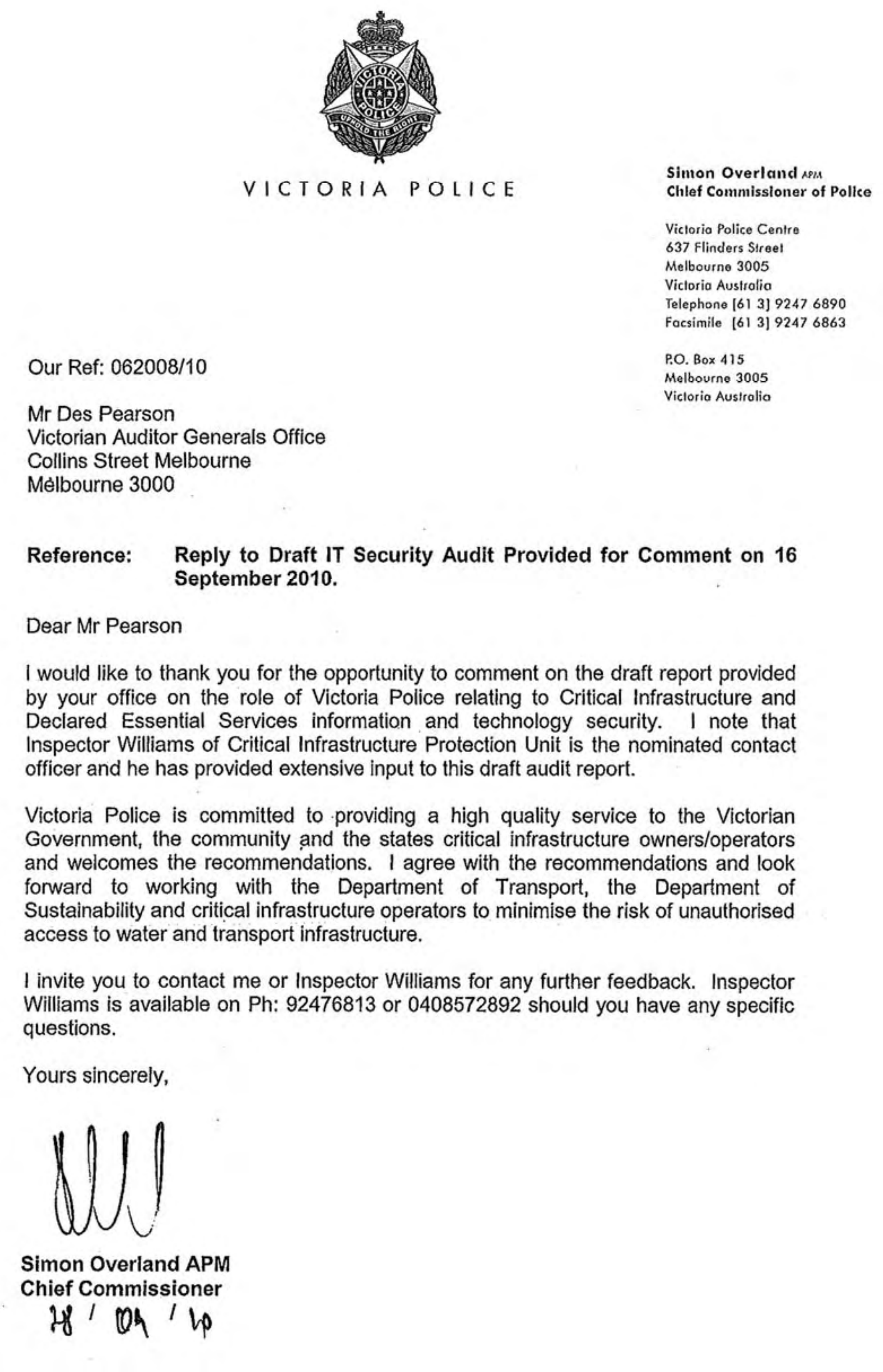
Yours sincerely

Greg Wilson
Secretary

Privacy Statement
Any personal information about you or a third party in your correspondence will be protected under the provisions of the ***Information Privacy Act 2000****. It will only be used or disclosed to appropriate Ministerial, Statutory Authority, or departmental staff in regard to the purpose for which it was provided, unless required or authorised by law. Enquiries about access to information about you held by the Department should be directed to the Manager Privacy, Department of Sustainability & Environment, PO Box 500, East Melbourne, 3002.*

Victoria
The Place To Be

RESPONSE provided by the Chief Commissioner, Victoria Police



VICTORIA POLICE

Simon Overland APM
Chief Commissioner of Police

Victoria Police Centre
637 Flinders Street
Melbourne 3005
Victoria Australia
Telephone [61 3] 9247 6890
Facsimile [61 3] 9247 6863

P.O. Box 415
Melbourne 3005
Victoria Australia

Our Ref: 062008/10

Mr Des Pearson
Victorian Auditor Generals Office
Collins Street Melbourne
Melbourne 3000

Reference: Reply to Draft IT Security Audit Provided for Comment on 16 September 2010.

Dear Mr Pearson

I would like to thank you for the opportunity to comment on the draft report provided by your office on the role of Victoria Police relating to Critical Infrastructure and Declared Essential Services information and technology security. I note that Inspector Williams of Critical Infrastructure Protection Unit is the nominated contact officer and he has provided extensive input to this draft audit report.

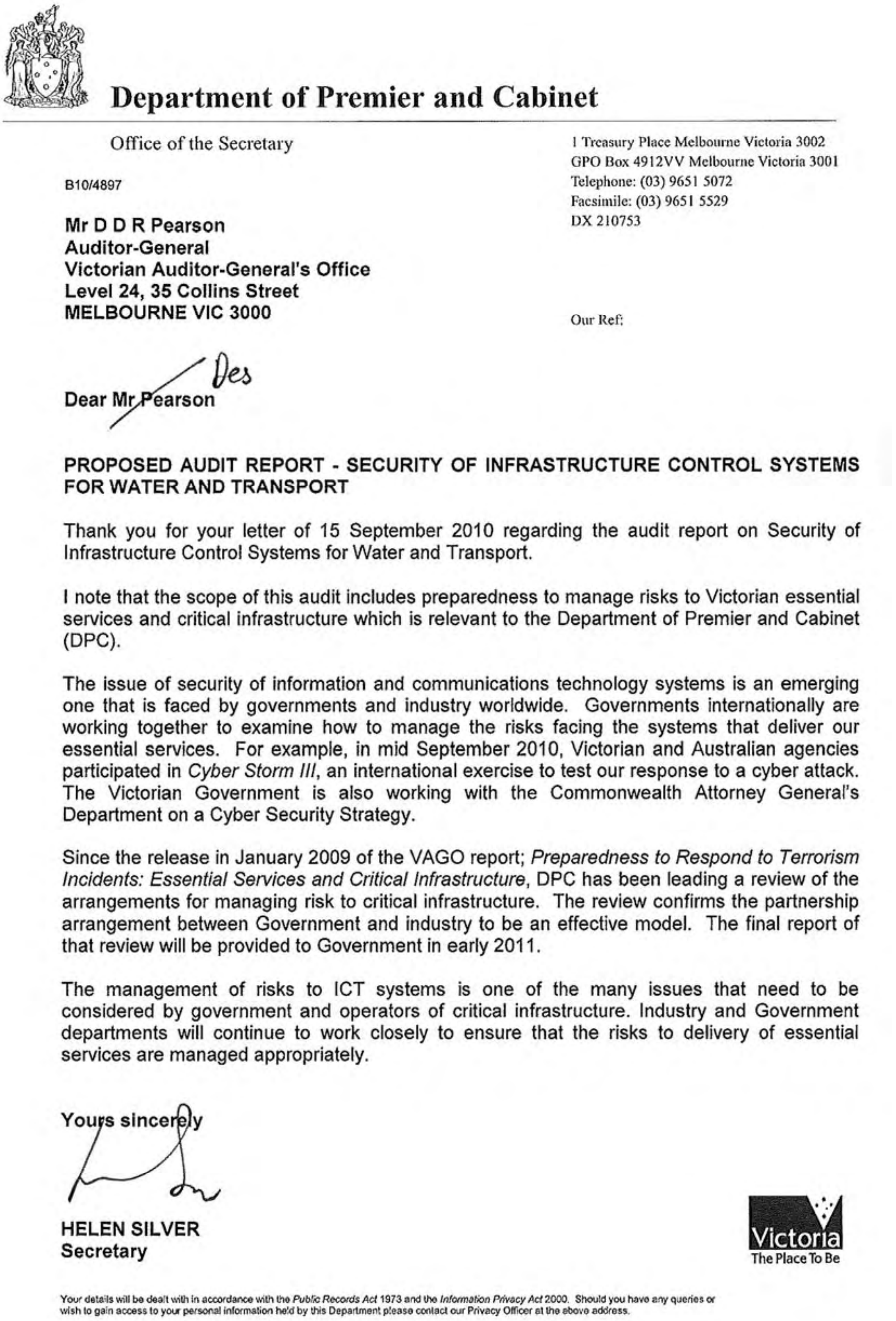
Victoria Police is committed to providing a high quality service to the Victorian Government, the community and the states critical infrastructure owners/operators and welcomes the recommendations. I agree with the recommendations and look forward to working with the Department of Transport, the Department of Sustainability and critical infrastructure operators to minimise the risk of unauthorised access to water and transport infrastructure.

I invite you to contact me or Inspector Williams for any further feedback. Inspector Williams is available on Ph: 92476813 or 0408572892 should you have any specific questions.

Yours sincerely,

Simon Overland APM
Chief Commissioner
28 / 09 / 10

RESPONSE provided by the Secretary, Department of Premier and Cabinet



Department of Premier and Cabinet

Office of the Secretary

1 Treasury Place Melbourne Victoria 3002
GPO Box 4912VV Melbourne Victoria 3001
Telephone: (03) 9651 5072
Facsimile: (03) 9651 5529
DX 210753

B10/4897

Mr D D R Pearson
Auditor-General
Victorian Auditor-General's Office
Level 24, 35 Collins Street
MELBOURNE VIC 3000

Our Ref:

Dear ~~Mr Pearson~~ Des

PROPOSED AUDIT REPORT - SECURITY OF INFRASTRUCTURE CONTROL SYSTEMS FOR WATER AND TRANSPORT

Thank you for your letter of 15 September 2010 regarding the audit report on Security of Infrastructure Control Systems for Water and Transport.

I note that the scope of this audit includes preparedness to manage risks to Victorian essential services and critical infrastructure which is relevant to the Department of Premier and Cabinet (DPC).

The issue of security of information and communications technology systems is an emerging one that is faced by governments and industry worldwide. Governments internationally are working together to examine how to manage the risks facing the systems that deliver our essential services. For example, in mid September 2010, Victorian and Australian agencies participated in *Cyber Storm III*, an international exercise to test our response to a cyber attack. The Victorian Government is also working with the Commonwealth Attorney General's Department on a Cyber Security Strategy.

Since the release in January 2009 of the VAGO report; *Preparedness to Respond to Terrorism Incidents: Essential Services and Critical Infrastructure*, DPC has been leading a review of the arrangements for managing risk to critical infrastructure. The review confirms the partnership arrangement between Government and industry to be an effective model. The final report of that review will be provided to Government in early 2011.

The management of risks to ICT systems is one of the many issues that need to be considered by government and operators of critical infrastructure. Industry and Government departments will continue to work closely to ensure that the risks to delivery of essential services are managed appropriately.

Yours sincerely

HELEN SILVER
Secretary

Victoria
The Place To Be

Your details will be dealt with in accordance with the *Public Records Act* 1973 and the *Information Privacy Act* 2000. Should you have any queries or wish to gain access to your personal information held by this Department please contact our Privacy Officer at the above address.

Auditor-General’s reports

Reports tabled during 2010–11

Report title	Date tabled
Portfolio Departments: Interim Results of the 2009–10 Audits (2010–11:1)	July 2010
Taking Action on Problem Gambling (2010–11:2)	July 2010
Local Government: Interim Results of the 2009–10 Audits (2010–11:3)	August 2010
Water Entities: Interim Results of the 2009–10 Audits (2010–11:4)	August 2010
Public Hospitals: Interim Results of the 2009–10 Audits (2010–11:5)	September 2010
Business Continuity Management in Local Government (2010–11:6)	September 2010
Sustainable Farm Families Program (2010–11:7)	September 2010
Delivery of NURSE-ON-CALL (2010–11:8)	September 2010
Management of Prison Accommodation Using Public Private Partnerships (2010–11:9)	September 2010
Soil Health Management (2010–11:10)	October 2010
Sustainable Management of Victoria's Groundwater Resources (2010–11:11)	October 2010
The Department of Human Services’ Role in Emergency Recovery (2010–11:12)	October 2010
Access to Ambulance Services (2010–11:13)	October 2010
Management of the Freight Network (2010–11:14)	October 2010

VAGO’s website at <www.audit.vic.gov.au> contains a comprehensive list of all reports issued by VAGO. The full text of the reports issued is available at the website.

VAGO
Victorian Auditor-General's Office
Auditing in the Public Interest

Availability of reports

Copies of all reports issued by the Victorian Auditor-General's Office are available from:

- Information Victoria Bookshop
  505 Little Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: 1300 366 356 (local call cost)
  Fax: +61 3 9603 9920
  Email: <bookshop@diird.vic.gov.au>

- Victorian Auditor-General's Office
  Level 24, 35 Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: +61 3 8601 7000
  Fax: +61 3 8601 7010
  Email: <comments@audit.vic.gov.au>
  Website: <www.audit.vic.gov.au>