Security of Critical Infrastructure Control Systems for Trains

Victorian Auditor-General's Report | November 2016 | 2016–17:6

VICTORIA

Victorian
Auditor-General

Security of Critical Infrastructure Control Systems for Trains

Ordered to be published

VICTORIAN
GOVERNMENT PRINTER
November 2016

PP No 219, Session 2014–16

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis (LCA) for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 55% recycled content.

ISBN 978 1 925226 72 0

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

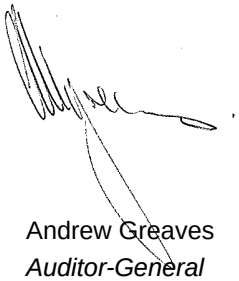
The Hon Bruce Atkinson MLC
President
Legislative Council
Parliament House
Melbourne

The Hon Telmo Languiller MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report on the audit *Security of Critical Infrastructure Control Systems for Trains*.

Yours faithfully



Andrew Greaves
Auditor-General

9 November 2016

Contents

Audit overview

Passenger train services for the Victorian public are an essential service, much like electricity, water, gas and port services. Train services rely on a range of systems and equipment, including control systems that monitor and control service delivery.

The capacity to continually deliver essential services depends on a number of factors, including effective computer system security controls and procedures that prevent unauthorised access or that detect and respond to security breaches. Failing to keep control systems secure can disrupt the delivery of essential services.

As cyber attacks become increasingly automated and sophisticated, control systems are more vulnerable. The move away from standalone control systems to those that are connected with other computer systems and networks also increases exposure to cyber attacks. We examined the security of train operators' control systems and Public Transport Victoria's (PTV) oversight of these operators.

Conclusion

In our 2010 audit *Security of Infrastructure Control Systems for Water and Transport*, we noted significant weaknesses in the security of control systems of water and train operators, and we made recommendations to address those weaknesses.

We reviewed the control systems of train operators and PTV's oversight of their performance. There has been little improvement since 2010, and significant weaknesses remain. If security vulnerabilities in control systems are not addressed, they may result in:

- extended or complete loss of train services
- economic loss to train operators and the Victorian economy
- reputational damage to train operators
- train operators losing control of commercial or sensitive information
- criminal damage or sabotage to control systems.

PTV and train operators' management of control systems' security continues to be weak. There are four key reasons for their lack of progress:

- poor governance arrangements and a lack of management oversight of control systems
- limited security frameworks for PTV's and train operators' control systems
- limited security controls for identifying, preventing, detecting and responding to cyber security events
- poor transfer of accountability and risk during machinery-of-government changes.

During this audit, the Acting Auditor-General gave written information to relevant ministers and a relevant head of a department for urgent investigation or attention, under section 16F of the *Audit Act 1994*. As required under this section, we also notified the Premier.

Findings

Governance of control systems

PTV has not adequately developed governance arrangements to oversee, monitor and support train operators to manage risks to their control systems. This has resulted in:

- incomplete and inadequate cyber security frameworks in train operators
- a lack of clarity and understanding between PTV and train operators about ownership, roles and responsibilities
- no strategic direction to develop minimum security requirements for control systems
- inadequate risk and compliance management processes
- limited progress in addressing the findings of our 2010 audit *Security of Infrastructure Control Systems for Water and Transport.*

PTV has not identified, prioritised or managed emerging risks to Victoria's essential train services and vulnerabilities of control systems.

PTV has not assigned roles and responsibilities for managing security of control systems in franchise and service agreements with train operators. This has resulted in a lack of clarity and understanding about the ownership of control systems, leading to some activities to secure these systems overlapping and others being omitted.

During the audit, we noted that PTV has started developing governance arrangements, systems and processes that aim to address our audit findings and recommendations.

Security frameworks for control systems

Train operators do not have the necessary security frameworks in place to safeguard the control systems that manage and monitor train services.

When we conducted the audit, PTV had not coordinated or provided guidance to train operators in its role as the public transport development authority responsible for the security of train control systems.

PTV has started to work with train operators to address our audit findings and implement improvements to ensure that control systems are more reliable.

Cyber security controls

Due to inadequate security frameworks, train operators do not have proper controls in place to secure their control systems. They have limited controls to identify, prevent, detect and respond to cyber security incidents. PTV and train operators recognise this situation and are developing strategies to address it.

Many of the detailed findings from this audit about the security of control systems are sensitive, and it is not in the public interest for us to include them in this report.

During the audit, the Acting Auditor-General issued management letters to PTV, sharing our findings and seeking assurance that consequent risks had been identified, assessed and where necessary that risk management processes have been put in place. The Acting Auditor-General asked PTV to engage with train operators to identify remediation actions and specified time frames for these actions. PTV responded, outlining its intended actions and time frames.

PTV and train operators are working cooperatively, and we will periodically examine whether these weaknesses are being addressed within an acceptable time frame. We may report to Parliament at a later date on their progress.

Machinery-of-government changes

Since our 2010 audit, machinery-of-government changes have transferred accountability for train control systems and the responsibility for resolving the recommendations from our 2010 audit.

On 27 June 2016, the Victorian Government announced that a new agency called Transport for Victoria (TFV) will be established in late 2016. TFV will have overarching responsibility for transport across Victoria and will be part of the Department of Economic Development, Jobs, Transport & Resources. Its role will include planning, coordinating and managing Victoria's transport networks as one system. PTV and Roads Corporation of Victoria (VicRoads) will be part of TFV.

We recommend the Department of Economic Development, Jobs, Transport & Resources consider the transfer of accountability and risk during machinery-of-government changes.

Recommendations

We recommend that Public Transport Victoria:

1. formalise governance arrangements with train operators and determine responsibilities for the cyber security of control systems (see Section 2.3.2)
2. prepare a cyber security strategy for control systems that establishes:
   - the desired level of security
   - governance arrangements that ensure adequate oversight

   (see Section 2.3.1)
3. include in the renegotiated franchise and service agreements with train operators:
   - a clarification of ownership, roles and responsibilities for the management and operation of control systems
   - requirements for the management of control system security

   (see Sections 2.3.3 and 2.3.4)
4. establish funding arrangements for control system upgrades, renewals and maintenance as part of the renegotiation of franchise and service agreements (see Section 2.3.5)
5. identify and appoint a team of suitably qualified and experienced professionals to provide advice to the train operators on security, risk and business continuity management (see Sections 2.3.2 and 2.6)
6. establish appropriate processes for accountability, tracking, management and reporting of their actions and train operators' actions, in response to audit recommendations (see Section 2.6)
7. advise train operators on how to implement appropriate risk management systems that identify, measure and monitor control system risks, by:
   - setting up a risk register
   - performing a risk analysis of identified security vulnerabilities to determine whether to immediately introduce security controls and/or technical fixes
   - applying the Victorian Government Risk Management Framework to consider inter-agency and relevant significant risks to Victoria

   (see Section 2.5.1)
8. advise train operators on how to implement appropriate compliance management systems that include:
   - processes to monitor, measure, evaluate and report on the performance of security controls
   - internal audit programs to regularly carry out vulnerability assessments or security tests to validate train operators' control system security

   (see Sections 2.5.2 and 2.5.3).

Recommendations – *continued*

We recommend that Public Transport Victoria:

9. set up a security controls framework that aims to identify, detect, prevent and respond to cyber threats and that:
    - clearly defines minimum requirements and key performance indicators
    - references the *Victorian Protective Data Security Framework*, *Victorian Protective Data Security Standards* and the security architecture that train operators should use for their respective control system environments
    - includes requirements for monitoring and reporting security incidents
    - includes a schedule of audits that Public Transport Victoria will carry out to monitor how the security controls framework is applied and managed
    - requires staff training in security of control systems
    - includes guidelines for sharing information with train operators to improve the security of control systems

    (see Sections 2.2, 2.3.6, 2.5.3 and 3.2).

We recommend that the Department of Economic Development, Jobs, Transport & Resources:

10. establish appropriate processes to manage the transfer of accountability and responsibility of recommendations (see Section 2.6).

Responses to recommendations

We have professionally engaged with the Department of Economic Development, Jobs, Transport & Resources, Public Transport Victoria (PTV), train operators, Victorian Rail Track and Emergency Management Victoria throughout the audit. In accordance with section 16(3) of the *Audit Act 1994* we provided a copy of this report or relevant extracts to those agencies and requested their submissions and comments. We also provided a copy of the report to the Department of Premier & Cabinet.

The following is a summary of those responses. The full responses are included in Appendix A.

The Department of Economic Development, Jobs, Transport & Resources and PTV responded, accepting the recommendations. PTV provided a detailed action plan on how it has begun to address our recommendations and the time frames for these activities. The Department of Justice & Regulation (on behalf of Emergency Management Victoria) and V/Line Proprietary Limited responded, noting the findings in the report. V/Line Proprietary Limited also noted that it will work closely with PTV to ensure that the recommendations are delivered within agreed time frames.

1 Audit context

1.1 Introduction

Passenger train services for the Victorian public are an essential service, much like electricity, water, gas and port services. Train services rely heavily on control systems that monitor and control service delivery. These control systems consist of:

- operational systems for metropolitan and regional passenger train services
- infrastructure management systems that control and monitor assets and power distribution
- passenger and operator safety systems, including closed-circuit television and passenger communication and information systems
- telecommunications and network infrastructure, including signalling systems and radio communications.

Control systems must be secure to ensure that Victoria's train services are sustainable, protected from unauthorised access and can be reliably operated and delivered. A breach in the security of control systems could result in disruption to train services.

In Victoria, several agencies are involved in managing and operating the train system, including the transport division of the Department of Economic Development, Jobs, Transport & Resources, Public Transport Victoria (PTV), and train operators Metro Trains Melbourne Proprietary Limited (MTM) and V/Line Proprietary Limited (V/Line). Victorian Rail Track (VicTrack) owns Victoria's train infrastructure, land and assets.

1.2 Train sector overview

1.2.1 Responsibility for the transport portfolio

Since our 2010 audit *Security of Infrastructure Control Systems for Water and Transport*, machinery-of-government changes have transferred responsibility for the transport portfolio multiple times:

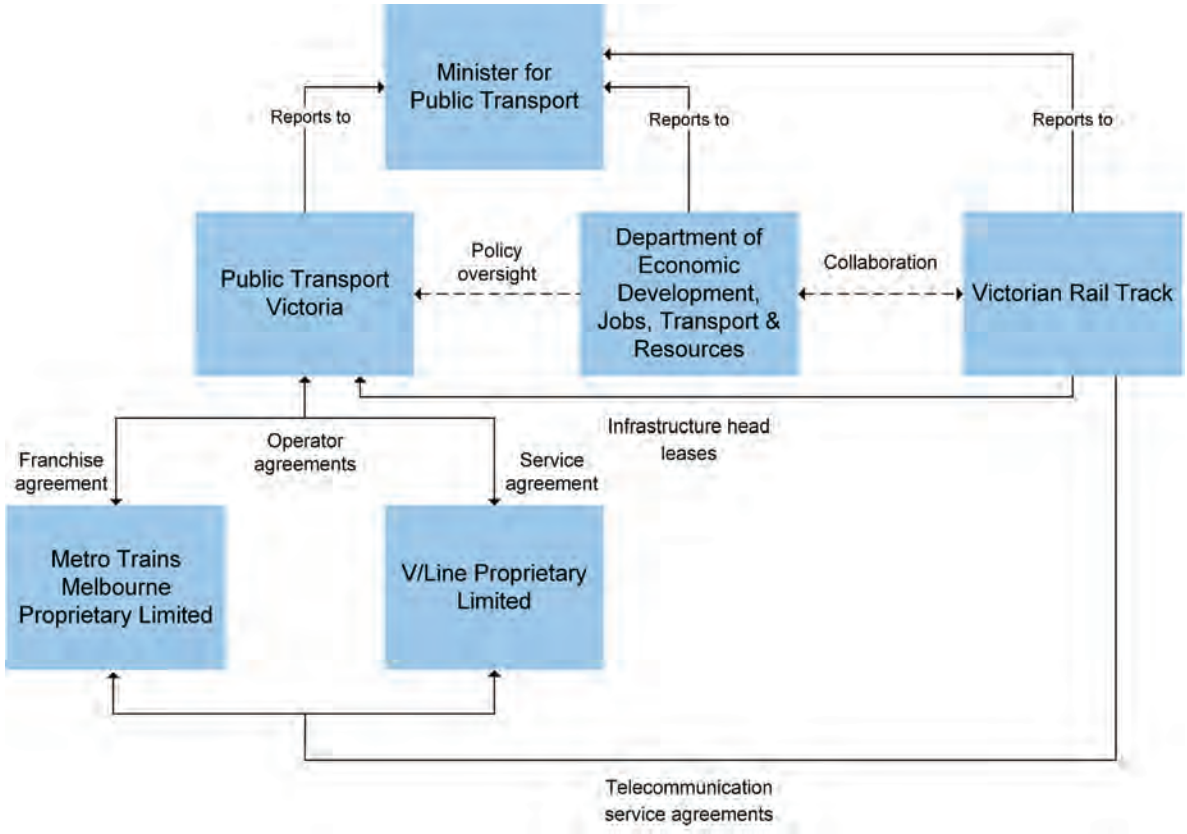
- In April 2013, responsibility for transport passed from the former Department of Transport (which had been the subject of our 2010 audit) to the Department of Transport, Planning & Local Infrastructure.
- From 1 January 2015, the Department of Economic Development, Jobs, Transport & Resources (the department) took responsibility for the planning and oversight of Victoria's transport system, infrastructure and services.

- On 27 June 2016, the Victorian Government announced that a new agency called Transport for Victoria (TFV) will be established in late 2016. TFV will have overarching responsibility for transport across Victoria and will be part of the department. Its role will include planning, coordinating and managing Victoria's transport networks as one system. PTV and Roads Corporation of Victoria (VicRoads) will be part of TFV.

1.2.2 Transport agencies

Figure 1A shows the relationship between the Minister for Public Transport and transport agencies.

Figure 1A
Relationship between the Minister for Public Transport and transport agencies



Note: In view of the impending establishment of TFV, this diagram is accurate as of 6 September 2016.
Source: VAGO.

The Department of Economic Development, Jobs, Transport & Resources

The department has overall responsibility for the planning, delivery and oversight of Victoria's transport system, infrastructure and services. It oversees transport regulatory policy and legislation. The department is also engaged in delivering the Victorian Government's major transport projects and initiatives to improve public and private transport and other major infrastructure in urban and rural Victoria.

Public Transport Victoria

PTV is the statutory authority responsible for planning, coordinating, providing, operating and maintaining a safe, punctual, reliable and clean public transport system—including train services. In November 2011, the *Transport Integration Act 2010* was amended to form PTV. On 2 April 2012, PTV began operation and assumed responsibilities for overseeing train operations previously exercised by the Director of Public Transport and the Department of Transport.

PTV delivers train services through its agreements with operators:

- MTM, which operates metropolitan train services in Victoria through a franchise agreement (a legally binding contract)
- V/Line, which operates regional train services in Victoria through a service agreement (as the legislated train operator).

The train operators use control systems to manage and control infrastructure to deliver train services across the train network.

Metro Trains Melbourne Proprietary Limited

MTM is the franchise operator of Victoria's metropolitan train service. It is a joint venture between the Hong Kong-based MTR Corporation, John Holland Group and UGL Rail. It operates 210 six-carriage trains across 869 kilometres of track. The train fleet provides more than 228 million train trips each year and transports 415 000 customers each day.

MTM is not an authority (a department, public body or an entity of which the state or a public body has control) and has participated voluntarily in this performance audit under section 15 of the *Audit Act 1994*.

V/Line Proprietary Limited

V/Line is a Victorian Government statutory authority legislated under the *Transport Integration Act 2010.* Its primary objective is to provide passenger and freight train services, and it is the sole provider of train and bus services in regional Victoria. In 2014–15, more than 15 million train and bus passenger trips were taken on V/Line services. Every week, more than 1 700 train services are scheduled between Melbourne and major regional cities.

1.2.3 Other agencies

Victorian Rail Track

VicTrack is the custodial owner of Victoria's train infrastructure, land and assets. It owns and operates the telecommunications infrastructure that supports Victorian metropolitan and regional train services. Train and telecommunications infrastructure and assets are leased via PTV to the train operators, except those owned by the train operators. VicTrack provides managed telecommunications services direct to the train operators via the telecommunications service agreements.

Emergency Management Victoria

In July 2014, Emergency Management Victoria (EMV) was formed when the *Emergency Management Act 2013* came into effect. EMV plays a key role in implementing the Victorian Government's emergency management reform agenda and developing a whole-of-government policy for emergency management. As of 1 July 2015, the 2014 amendment to the *Emergency Management Act 2013* requires operators of critical infrastructure declared vital to create emergency risk management plans.

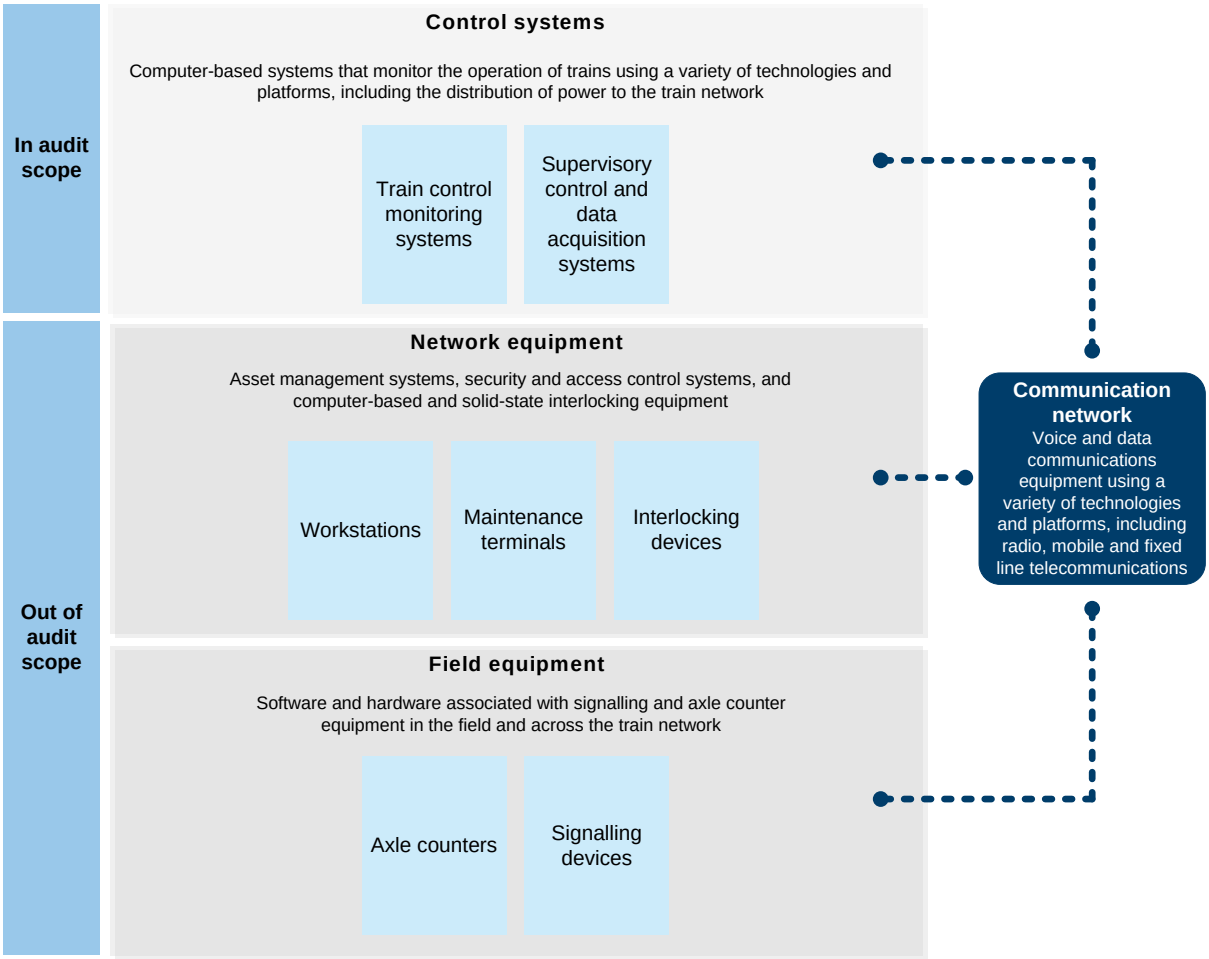
EMV also supports the Emergency Management Commissioner, who has overall responsibility for coordination and response before, during and after major emergencies, including managing the consequences of an emergency that affects critical infrastructure. This role was previously performed by Victoria Police under the *Terrorism (Community Protection) Act 2003*.

1.3 Control systems overview

Critical infrastructure for train services includes network equipment, field equipment and the communication network, which are all monitored and controlled by control systems. These systems are computer based and are assets that should be managed across their life cycle to support the delivery of train services. Control systems must be secure to ensure that train services are sustainable and protected from unauthorised access and can also be reliably operated and delivered.

This audit specifically focused on the security of control systems. Figure 1B shows the boundary between control systems, network equipment, field equipment and the communication network.

Figure 1B
Relationship between control systems, network equipment, field equipment and the communication network



Source: VAGO.

1.3.1 Risks to control systems

Cyber attacks pose a growing threat to the security of control systems. Australia's Trusted Information Sharing Network—a forum established by the Australian Government to build the resilience of critical infrastructure for business and government—advised that the risk of cyber attack is escalating, with targeted attacks having the capability to damage infrastructure.

For Victoria's train system, if security vulnerabilities in control systems are not addressed, they may result in:

- extended or complete loss of train services
- economic loss to train operators and the Victorian economy
- reputational damage to train operators
- train operators losing control of commercial or sensitive information
- criminal damage or sabotage to control systems.

As cyber attacks become increasingly automated and sophisticated, control systems become more vulnerable. The move away from standalone control systems to those that are connected with other computer systems and networks also increases their exposure to cyber attacks.

The motivation for launching a cyber attack varies, but it typically includes a desire to cause harm, to demand a ransom, to cause service disruption, to inflict reputational damage or to steal data. The possibility of trusted users such as employees, vendors and external contractors accessing or operating control systems inappropriately, causing service disruption, poses another threat.

Figure 1C defines key terms in this report.

Figure 1C
Key definitions

Term	Definition
Cyber threat	The threat of unauthorised access to a control system device and/or network. This access could be directed from within an organisation (for example, by a disgruntled employee) or from a remote location by an unknown person (for example, a hostile government, a terrorist group or a malicious intruder) using the internet.
Cyber attack	A deliberate act through the internet to manipulate, deny, degrade or destroy computers or networks, or the information stored in them. The objective of a cyber attack is to seriously compromise security, stability or prosperity.
Hostile actor	An individual or organisation—including an agency of a nation state—that conducts cyber attacks.

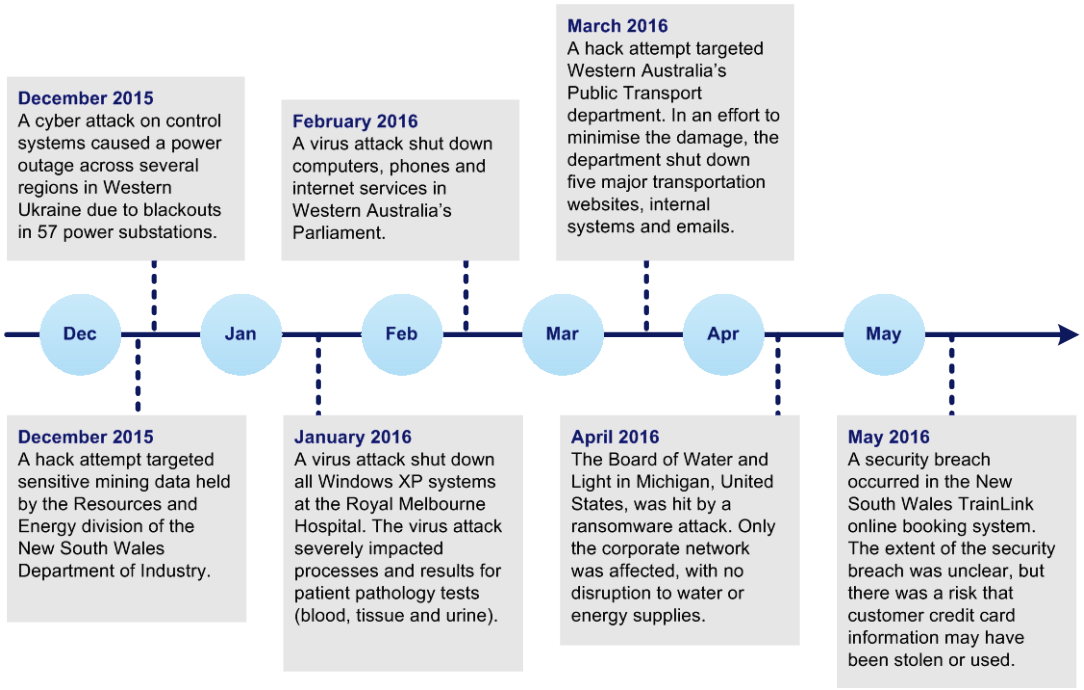
Source: VAGO.

In 2014–15, CERT Australia—the Australian Government's national computer emergency response team, a partner agency of the Australian Cyber Security Centre—responded to 11 733 incidents affecting Australian organisations, 218 of which involved systems of national interest and critical infrastructure. A CERT Australia survey in 2015 asked respondents a series of questions about cyber attacks. The survey's results indicated that:

- 72 per cent of respondents had experienced an attack by ransomware—malicious software designed to block access to a system until a sum of money is paid
- 60 per cent of respondents saw trusted insiders as the most concerning hostile actor, followed by motivated groups or hackers at 55 per cent, and organised criminal syndicates at 54 per cent.

Figure 1D shows some examples of cyber attacks across different industries reported globally since December 2015.

Figure 1D
Reported cyber attacks



Source: VAGO.

1.4 Legislative and policy context

Transport Integration Act 2010

The *Transport Integration Act 2010* came into effect on 1 July 2010 and is Victoria's primary transport act. The *Transport Integration Act 2010* requires that all decisions affecting the transport system be made within the same integrated decision-making framework and support the same objectives. A 2011 amendment to the *Transport Integration Act 2010* created PTV.

Rail Safety Act 2006

The *Rail Safety Act 2006* came into effect on 1 August 2006 and is the prime statute legislating the safety of rail operations in Victoria. The *Rail Safety Act 2006* forms part of the transport policy and legislation framework in Victoria.

Emergency Management Act 2013

The *Emergency Management Act 2013* came into effect on 1 July 2014 and established governance arrangements for emergency management in Victoria. The governance arrangements require all government agencies and other organisations to work collaboratively to respond to any potential or existing situation that may cause harm to people or damage to property or the environment. As of 1 July 2015, the 2014 amendment to the *Emergency Management Act 2013* requires operators of critical infrastructure declared vital to create emergency risk management plans.

Critical Infrastructure Resilience Strategy

The 2015 *Critical Infrastructure Resilience Strategy* sets out the vision, principles and strategic priorities for building the resilience of Victoria's critical infrastructure. It highlights cyber attack as one of the emergency risks that critical infrastructure owners and operators should prepare for.

Victorian Protective Data Security Framework

In July 2016, the *Victorian Protective Data Security Framework* (VPDSF) and *Victorian Protective Data Security Standards* (VPDSS) were published by the Commissioner for Privacy and Data Protection. The VPDSF and VPDSS establish mandatory requirements to protect public sector data and provide for governance across the four domains of information, personnel, information and communication technology (ICT) and physical security. PTV and train operators are required to comply with the VPDSF and VPDSS requirements by July 2018.

Asset Management Accountability Framework

The *Asset Management Accountability Framework* was released by the Department of Treasury & Finance in February 2016. The framework establishes a set of mandatory requirements and general guidance to ensure Victorian public sector agencies manage assets appropriately. This includes ICT assets.

Information Technology Strategy: Victorian Government 2016–2020

The *Information Technology Strategy: Victorian Government 2016–2020* was released by the Department of Premier & Cabinet in May 2016. The strategy provides direction for government on information management and technology for the next five years, including development of a statement of direction and overall strategy for cyber security.

1.5 Standards

The following standards include relevant principles for good governance and information security policy:

- ISO/IEC 27001:2013 Information Security Management
- ISO/IEC 21827:2008 Systems Security Engineering—Capability Maturity Model
- ISA/IEC 62443 Standard Suite for Industrial Automation and Control Systems
- AS/NZS ISO 31000:2009 Risk Management.

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

- Security Benchmarks, Center for Internet Security (United States) <https://benchmarks.cisecurity.org>
- *Catalog of Controls Systems Security,* version 7, April 2011, Department of Homeland Security (United States)
- *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0, February 2014, National Institute of Standards and Technology (United States)
- NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology (United States)
- *Sherwood Applied Business Security Architecture*, SABSA (United Kingdom) <http://www.sabsa.org>.

1.6 Why this audit is important

Passenger train services are an essential service for the Victorian public. Train services rely heavily on control systems that monitor and control service delivery. Control systems must be secure to ensure that Victoria's train services are sustainable, protected from unauthorised access and can be reliably operated and delivered. A breach in the security of control systems could result in disruption to train services.

1.7 Previous audits

In October 2010, we tabled the performance audit report *Security of Infrastructure Control Systems for Water and Transport*. We found that the risk of unauthorised access to water and transport infrastructure control systems was high. Unauthorised access could compromise these systems and affect the stable delivery of essential services to the community.

In November 2013, we tabled the performance audit report *Whole-of-Victorian-Government Information Security Management Framework*. We found that policy, standards and protection mechanisms for the security of information and communications technology systems and data across 11 public sector agencies had not been effectively applied.

1.8 What this audit examined and how

Our objective was to assess whether security risks to critical infrastructure control systems that operate and control train services are managed effectively. To do this, we assessed whether:

- appropriate levels of governance over control systems have been established
- processes and controls to identify, prevent, detect and respond to security events in control systems are effective
- business continuity and disaster recovery capabilities are effective and there are established response capabilities
- transport agencies have implemented recommendations raised in our 2010 audit *Security of Infrastructure Control Systems for Water and Transport*.

We focused on metropolitan and regional train services for two reasons:

- the high-volume of patronage—in 2014, train services accounted for approximately 236 million passenger trips, which is 45 per cent of total public transport usage in Victoria
- the potential impact that a security breach or disaster would cause to public transport services and safety.

The audit includes the department, agencies and train operators involved in the provision of passenger train services to the Victorian public:

- Department of Economic Development, Jobs, Transport & Resources
- Public Transport Victoria
- Metro Trains Melbourne
- V/Line Proprietary Limited
- Victorian Rail Track
- Emergency Management Victoria.

We conducted this audit in accordance with section 15 of the *Audit Act 1994* and Australian Auditing and Assurance Standards. The total cost of this audit was $545 000.

In accordance with section 20(3) of the *Audit Act 1994*, we express no adverse comment or opinion about anyone we name in this report.

1.9 Report structure

This report is structured as follows:

- Part 2 examines whether appropriate levels of governance over control systems have been established and the extent to which transport agencies have implemented recommendations raised in our 2010 audit *Security of Infrastructure Control Systems for Water and Transport.*
- Part 3 examines whether processes and controls to identify, prevent, detect and respond to security events in control systems are effective.

2 Governance of control systems

Under the *Transport Integration Act 2010*, Public Transport Victoria (PTV) is responsible for planning, coordinating, providing, operating and maintaining a safe public transport system, including train services. PTV, train operators and other relevant entities have a shared responsibility under the *Rail Safety Act 2006* to make sure train services are safe. This includes securing control systems—the central systems that manage and monitor train services.

PTV is the public transport development authority responsible for establishing governance arrangements to oversee the development of a coordinated cyber security strategy and making sure the strategy is delivered. Effective cyber security relies on full engagement at all levels of PTV, train operators and other relevant entities—including a responsibility for boards to set a cyber security strategy and ensure it is implemented.

Middle and front-line management in PTV, train operators and other relevant entities play an important role in delivering the cyber security strategy through day-to-day operations. They also play a vital role by providing feedback to PTV and their executive management teams.

During public transport disruptions, PTV, with the assistance of train operators, is responsible for ensuring the restoration of train services. During a major emergency, the Emergency Management Commissioner is responsible for overseeing the response and recovery arrangements, and managing the impacts of the emergency on critical infrastructure.

2.1 Conclusion

PTV has not adequately established governance arrangements to oversee the management of control systems, resulting in:

- incomplete and inadequate cyber security frameworks in train operators
- a lack of clarity and understanding between PTV and train operators about ownership, roles and responsibilities for the management and operation of control systems
- no strategic direction or coordination of train operators to develop consistent minimum security requirements for control systems
- inadequate risk and compliance management processes
- limited progress in addressing the findings of our 2010 audit *Security of Infrastructure Control Systems for Water and Transport*.

We note that PTV has begun to establish governance processes, which will help it put actions in place to improve the security of train control systems.

2.2 Statutory oversight of cyber security

Our previous audits have highlighted inadequate cyber security in Victorian public sector agencies. The Department of Premier & Cabinet stated in the *Information Technology Strategy: Victorian Government 2016–2020* that the government must take a strategic approach to managing system security due to the escalating threat of cyber attacks.

Emergency Management Victoria commented in 2015, in its *Critical Infrastructure Resilience Strategy,* that cyber attacks are an emergency risk, and Victorian critical infrastructure owners and operators should prepare for them.

Despite the increasing importance of cyber security, transport agencies currently have limited guidance to support them in reducing their vulnerability to cyber attacks.

Legislative requirements

The *Transport Integration Act 2010* states that PTV is responsible for planning, coordinating, providing, operating and maintaining a safe, punctual, reliable and clean public transport system.

Safety management is well established in train services, as required under the *Rail Safety Act 2006*. Management of cyber security must be approached in a similar way, but there is no legislation that mandates cyber security requirements. Other countries have identified the need to address cyber security for train services and have developed specific guidelines, such as *Rail Cyber Security: Guidance to Industry*, produced by the United Kingdom's Department of Transport.

Policy and standards

Until recently, there were no mandatory policies or standards for managing cyber security. In July 2016, the Victorian Government released the *Victorian Protective Data Security Framework* (VPDSF) and *Victorian Protective Data Security Standards* (VPDSS). The VPDSF and VPDSS establish mandatory requirements for protecting public sector data and establish governance arrangements across the domains of information, personnel, information and communication technology (ICT) and physical security. PTV and train operators must comply with the VPDSF and VPDSS requirements by July 2018.

In August 2016, PTV notified train operators of the new requirements and offered annual compliance assessments of their control systems against the VPDSF and VPDSS. PTV requested train operators to:

- assign information security accountability to an executive director
- nominate subject matter experts on control system security
- undertake a security risk profile assessment by June 2017
- develop a protective data security plan by December 2017
- attest to their compliance with the VPDSF and VPDSS by December and June of each year.

Train operators have responded and nominated appropriate executive directors and subject matter experts.

The Rail Industry Safety and Standards Board (RISSB) is responsible for the development and management of rail industry standards in Australia. RISSB is developing a standard to manage control system security risks, which is expected to be published by December 2017. Victoria's train operators are both members of RISSB.

2.3 Public Transport Victoria responsibilities

Under the *Transport Integration Act 2010*, the main role of PTV is to deliver safe and reliable public transport services. In this role, it needs to effectively oversee the security of control systems by:

- setting up governance arrangements for PTV, train operators and other relevant entities
- defining, documenting and communicating the roles and responsibilities of staff, boards and committees involved in securing control systems
- assigning overall accountability for managing cyber security to a person or group
- regularly reporting to governing boards and committees on control systems and associated security risks.

2.3.1 Strategic direction

Under the *Transport Integration Act 2010*, PTV is required to develop and implement policies and strategies to improve the safety of passenger services and the security of the public transport system. We found that PTV has not yet developed a cyber security strategy for control systems.

In its *Information Technology Strategy: Victorian Government 2016–2020*, the government has committed to developing an overall strategy for cyber security by December 2016. This strategy will potentially contribute to the standardised, strategic and coordinated management of control systems.

2.3.2 Coordination and support

Before PTV was established, control systems were managed by the former Department of Transport's Systems and Information Services Division (SISD). Now that SISD has been disbanded, it is not clear who is responsible for managing and supporting control systems, and train operators' activities and projects for control systems have not been coordinated.

In our 2010 audit *Security of Infrastructure Control Systems for Water and Transport*, we recommended that a security team be set up by the former Department of Transport, comprising suitably qualified and experienced staff who could provide train operators with advice on managing security, risk and business continuity. In this audit, we noted that PTV has only one designated staff role with responsibility for these activities.

PTV has established a new Information and Controls Security Steering Committee, comprising executive management representatives from PTV and train operators. The committee met for the first time on 27 July 2016 but only one out of seven executive management representatives attended. Management from PTV, train operators and other relevant entities will need to be fully engaged and committed to make this committee and the cyber security strategy effective.

2.3.3 Control systems—ownership and responsibility

Control systems are an asset. They must be managed across their life cycle by the asset owner, to ensure they can deliver the intended service. The Victorian Government's February 2016 *Asset Management Accountability Framework* establishes a set of mandatory requirements and general guidance to ensure assets in the Victorian public sector are appropriately managed.

We identified a lack of understanding about the ownership of control system assets and responsibility for these assets. We noted instances where PTV, train operators and Victorian Rail Track (VicTrack) could not clearly show which agency owned and had responsibility over control systems. This has led to some activities overlapping and some being omitted, including:

- PTV and train operators duplicating frameworks, policies and procedures
- train operators duplicating engineering and maintenance support resources
- limited management of the security of control systems.

2.3.4 Franchise and service agreements

Train services are managed through franchise and service agreements between PTV and the two train operators. These agreements define PTV's responsibilities—including responsibilities that are contracted and/or legislated to train operators—and the requirements for train operators in the delivery of train services. By setting responsibilities and requirements, PTV and train operators can monitor and report on how they are managing and operating control systems, including security.

We reviewed the agreements between PTV and train operators and found that security of control systems is not included as a requirement. As a result, there are no minimum security standards for control systems that train operators need to implement and maintain.

PTV acknowledged this omission and will include control system security requirements in the renegotiated franchise and service agreements. The current service agreement for one train operator is due to expire in December 2016, and the franchise agreement for the other train operator is due to expire in November 2017. Both train operators are currently in negotiations with PTV.

2.3.5 Funding

The Victorian Government pays for the maintenance and upkeep of control systems through several funding streams based on activity and asset type. These streams include:

- **renewals of control systems**—continuous improvement projects to upgrade or enhance control systems are funded as individual projects outside of the franchise and service agreements
- **maintenance of control systems**—activities to repair and preserve the condition of control systems are funded through an annual funding pool under the infrastructure leases between PTV and train operators
- **ICT or business system upgrades**—activities to maintain minimum standards of business systems, which are sometimes used to support control systems and conventional office systems, are funded through an annual funding pool under the franchise and service agreements
- **telecommunications maintenance and upgrades**—partly funded by VicTrack's asset management program and partly paid directly by the train operators under the telecommunications service agreements with VicTrack.

The lack of clarity about which agency owns and has responsibility for control systems has resulted in maintenance of and upgrades to control systems not being a funding priority.

We noted that the Department of Economic Development, Jobs, Transport & Resources (the department) and PTV are reassessing funding options as part of the current renegotiation of franchise and service agreements between PTV and train operators.

2.3.6 Security framework, policies and procedures

A security framework is a series of documented policies and processes that are used to guide management and staff in performing their duties. These policies and procedures should reflect legislative requirements, government policy decisions, agreements and internal requirements. Train operators need to establish effective and comprehensive policies and procedures to secure the control systems they operate.

Under the *Transport Integration Act 2010*, PTV is required to develop and implement policies and strategies to improve the safety of passenger services and the security of the public transport system.

We note that before this audit PTV had not developed policies or provided guidance to train operators. Instead, we found that effort was being duplicated as train operators had independently started to develop security frameworks, policies and procedures, which were at varying stages of development.

During this audit, PTV has developed a security framework and prepared new security arrangements for train operators, but it has not yet provided formal advice to train operators about these arrangements.

PTV needs to adopt a centralised, coordinated approach to governance to encourage more effective collaboration between PTV and the train operators and set minimum security standards.

2.4 How train operators manage cyber security

2.4.1 Boards of PTV and train operators

Effective cyber security relies on full engagement by all levels of an entity—including a responsibility for the entity's board to set a cyber security strategy and ensure it is implemented.

We noted that the board of PTV has limited oversight of vulnerabilities, threats and risks to control systems. We identified:

- little evidence of reporting on cyber security issues to the board—PTV had only once provided high-level reporting about cyber security to its board, in April 2016
- limited board involvement in matters concerning the cyber security of control systems.

We also noted that one train operator regularly reports on control system security to its board while the other does not.

2.4.2 Executive management in PTV and train operators

To ensure that cyber security strategy and measures are implemented, all members of an entity must be committed to securing control systems. Security programs with a clear strategy, adequate funding and visible support from executive managers are more likely to function more effectively.

We found that there is no clear responsibility for providing direction or support for the cyber security of control systems at the executive management level within PTV.

Figure 2A provides an example of a cyber attack on Saudi Arabia's national oil and gas firm.

Figure 2A
Case study: Cyber attack on Saudi Aramco

On 15 August 2012, the computer network of Saudi Aramco—Saudi Arabia's national oil and gas company—was struck by a virus dubbed 'Shamoon', which infected up to 30 000 of its computers. Saudi Aramco took almost two weeks to recover from the damage.

The virus's main function was to indiscriminately delete data from computer hard drives. Although this did not result in an oil spill, explosion or other major fault in Saudi Aramco's operations, the attack affected the business processes of the company because every computer system was physically unplugged to prevent the virus from spreading further.

Without technology, Saudi Aramco had to manage supplies, shipping, payments and contracts with governments and business partners on paper. The company temporarily stopped selling oil to domestic gas tank trucks. After 17 days, the company relented and started giving oil away for free to keep it flowing within Saudi Arabia. Saudi Aramco's ability to supply 10 per cent of the world's oil was suddenly at risk.

The Shamoon virus also spread to the networks of other oil and gas company, including that of RasGas—Qatar's second biggest liquefied natural gas producer.

Source: VAGO, based on articles from the International Institute for Strategic Studies and Cable News Network.

2.5 Managing risk and compliance

Compliance and risk management are critical and interrelated components of an effective framework of standards and processes for safety and security management.

To manage risk, an entity must assess existing and potential risks, enabling it to mitigate and manage the impact of these risks by implementing new policies and procedures.

To manage compliance, an entity commits to acting within legislative requirements, policies and procedures, to ensure it is acting legally and ethically.

2.5.1 Risk management

Because control systems are the central systems that manage and monitor train movements, PTV and train operators need to have a clear understanding of the risks that may affect these systems, such as potential cyber attacks. The increasing sophistication of cyber attacks means that train control systems are increasingly vulnerable and require protection.

Train operators are required, under franchise and service agreements, to maintain a risk management system that complies with the Australian and New Zealand risk management standard AS/NZS ISO 31000:2009. The train operators had different approaches to assessing control system risks in their broader organisational risk management plans—one operator's plan included control system risks while the other's did not. We also noted that although PTV has a risk management plan, it does not address risks to control systems. This means that PTV and one of the train operators have no risk management strategies or risk registers for control systems.

During this audit, the Acting Auditor-General issued management letters to PTV, outlining a number of issues of concern that have not been included in this report due to their sensitive nature. The Acting Auditor-General recommended that PTV engage with train operators to identify and mitigate risks and address security vulnerabilities. PTV has begun to establish governance processes to address these risk management issues and improve the security of train control systems.

2.5.2 Compliance management

We reviewed the processes used by PTV and train operators to manage compliance. The processes were not robust enough for them to monitor, measure, evaluate and report compliance on performance measures related to control systems.

Train operators are independently identifying controls and requirements for compliance, and implementing processes to address them, without coordination from PTV. Compliance activities should be embedded in day-to-day operations, policies and procedures, but instead they are haphazard and uncoordinated.

Following recommendations from an internal audit, one train operator developed a compliance management framework and compliance obligations register in July 2016, and revised its compliance policy.

2.5.3 Monitoring risk and compliance

The *Transport Integration Act 2010* requires PTV to perform audits on public transport infrastructure assets, including control systems. By performing regular audits, PTV will be able to monitor the security of control systems as part of its responsibility to manage public transport infrastructure.

Train operators and PTV should be more active in undertaking audits on the security of control systems. Since its establishment, PTV has only carried out one audit, in January 2016, which evaluated the security framework for control systems of both train operators and itself. Train operators need to implement programs to regularly carry out vulnerability assessments and tests to assess the security of their control systems.

2.6 Management and resolution of audit findings and recommendations

In our 2010 audit, *Security of Infrastructure Control Systems for Water and Transport*, we made three key recommendations for transport agencies. These included reviewing and implementing security improvements to control systems and setting up a centralised security team to provide advice to train operators.

Since our 2010 audit, machinery-of-government changes have shifted accountability for train control systems and responsibility for resolving the recommendations from our audit. Without a clear process to manage these changes in accountability, the department and PTV could not provide assurance that detailed information from our 2010 audit had been communicated to the train operators. Further, the proposed centralised security team has not been set up.

3 Cyber security of control systems

Security risks to control systems have increased significantly in recent years. Around the world, public and private sector systems have faced unprecedented and escalating cyber threats to the security of information.

Global information security policies and standards are based on the International Organisation for Standardization ISO 27000 series of standards, which provide best practice recommendations on risks and controls as part of an overall information security management system. Other relevant industry standards include ISA/IEC 62443 from the International Society of Automation, and *NIST SP 800-53 Rev. 4*, published by the National Institute of Standards and Technology.

We assessed the two passenger train operators' cyber security of control systems against a security framework based on industry standards—a series of documented processes used to define policies and procedures for implementing and managing information security controls. We also looked at the security configuration of train operators' control systems.

3.1 Conclusion

The security frameworks that train operators have in place do not adequately safeguard the control systems that operate train services. The security controls used to identify, prevent, detect and respond to cyber threats are not able to prevent unauthorised access to the operators' control systems.

We identified serious security vulnerabilities in the control systems, which could expose them to cyber threats.

We notified Public Transport Victoria (PTV) and the train operators about the security vulnerabilities we identified, and they have accepted the identified weaknesses. The train operators have reviewed the security vulnerabilities and have either developed or are currently developing remediation plans to address these risks and weaknesses.

3.2 Cyber security framework

A cyber security framework defines the policies and procedures that an organisation uses to implement and manage its information security controls. The framework acts as a foundation for building an information security program that:

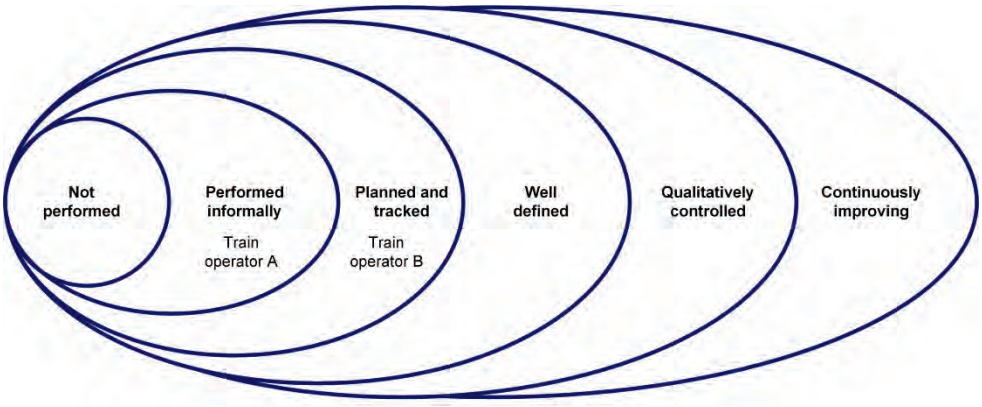
- mitigates risks
- reduces vulnerabilities
- defines and prioritises the tasks required to integrate cyber security into an entity.

Train operators' security over control systems was measured against the ISO/IEC 21827:2008 Systems Security Engineering—Capability Maturity Model. This model assesses the maturity of control system security on the following scale:

- **not performed**—incomplete processes
- **performed informally**—ad hoc processes and success that depend on individual efforts
- **planned and tracked**—plans developed and processes in place to track performance
- **well defined**—processes documented, standardised and integrated
- **qualitatively controlled**—processes are qualitatively measured, understood and controlled
- **continuously improving**—quantitative feedback used to continuously improve the process.

Figure 3A summarises the results of the assessment of train operators using this framework.

Figure 3A
Capability maturity model assessment



Source: VAGO.

The results indicate that train operators' security frameworks for control systems are at low levels of maturity. Specific elements assessed in the cyber security framework are discussed below.

Security awareness

Security awareness training is the formal process for educating employees about security. This training helps employees to apply organisational policies and procedures and alert managers to compliance matters and breaches. Security awareness training can foster a strong security culture through general awareness, education programs and staff training.

Train operators' security awareness training programs for physical security and general awareness are reasonable—enough training is in place to provide employees with a basic awareness of physical security matters and the appropriate responses to them.

However, we found that:

- train operators' security awareness training programs do not cover security of control systems
- there is little evidence of train operators preparing broader strategies to educate and raise employees' security awareness
- there are no forums to share knowledge about control systems between train operators and PTV.

Security monitoring

Security monitoring is a key process that enables train operators to detect and prevent security incidents. Intrusion detection systems monitor events on a network to identify unusual traffic patterns or changes to critical operating files. These events might include system or network activities such as login attempts or file access attempts. Intrusion prevention systems take intrusion detection one step further by automatically acting to stop detected cyber attacks.

Train operators should improve their ability to detect and prevent cyber attacks.

Service continuity and restoration

An effective control system has a 'high availability' requirement—it needs to be durable and likely to operate continuously without failure for a long time. One way for train operators to achieve high availability is to have emergency response and contingency plans they can execute during a disaster such as a system outage.

Emergency response and contingency plans provide information on how a specific business function or operating site can be re-established after a disaster, such as in an alternative operating location. These plans should be reviewed and updated and tested regularly to ensure that they continue to meet objectives.

Train operators should improve their emergency response and contingency plans as well as the capability of their disaster recovery sites.

User access management

User access management relates to managing access to systems, including how access is approved, revoked and periodically reviewed to ensure that it is in line with staff roles and responsibilities. The main objective of managing user access is to maintain the confidentiality, integrity and availability of systems and data.

Weaknesses in user access management controls can result in inappropriate and excessive privileges being assigned to users, which could give them unauthorised access to control systems.

Train operators should improve their user access management processes and controls to better restrict and manage which users can access their control systems.

Change management

The objective of change management is to ensure that changes to a computer system or its environment are appropriate and preserve the integrity of the underlying system and data. Weaknesses in change management can lead to an increased risk of unauthorised changes being made to systems and data, which could affect their availability and integrity.

Train operators should improve their change management processes and controls to better manage the integrity of control systems.

Patch management

A patch is an additional piece of software that vendors release to fix specific flaws in software or systems. Security vulnerabilities are flaws that can be exploited to gain unauthorised access to systems or to make inappropriate use of software. Periodic patching aims to improve the security of systems by reducing the number and likelihood of vulnerabilities being exploited.

Train operators should improve their patch management processes and controls to actively manage the vulnerabilities in their control systems, through periodic and timely patching.

3.3 Vulnerability assessment of control systems

Vulnerability assessment is a process that defines, identifies and classifies the security weaknesses in a computer system and tests its ability to identify, prevent, detect and respond to cyber attacks.

Figure 3B provides an example of a cyber attack on Ukrainian power companies.

Figure 3B
Case study: Cyber attack against Ukrainian critical infrastructure

On 23 December 2015, Ukrainian power companies experienced unscheduled power outages for several hours, affecting approximately 225 000 customers in Ukraine. This outage was caused by remote cyber attacks at three regional electric power distribution companies. Although power was eventually restored, all three regional electrical power distribution companies continue to run under constrained operations.

The cyber attacks were reportedly synchronised and coordinated—they occurred within 30 minutes of each other and impacted multiple central and regional facilities. During the cyber attacks, the hostile actors used remote administration tools to perform malicious remote operation of control systems and critical infrastructure. The companies believe that the hostile actors acquired legitimate credentials prior to the cyber attack to facilitate the remote access.

All three companies indicated that the hostile actors corrupted the systems at the conclusion of the cyber attack, rendering them inoperable. At the same time, the hostile actors overwhelmed the companies' call centres with automated telephone calls, affecting their ability to receive outage reports from customers and frustrating the companies' response efforts.

Source: VAGO, based on information from the United States Department of Homeland Security.

As part of this audit, we appointed an independent specialist to help carry out a vulnerability assessment of the train operators' control systems. The specialist evaluated the control systems' technical controls, and found several deficiencies in their security, mainly in network security, remote access security and legacy operating systems.

Network security

Network separation is one of the most effective ways an organisation can mitigate cyber threats. Separating networks can increase cyber security by reducing the number of connections within a computer system, which can deter or prevent access to critical resources and information.

Our vulnerability assessment showed that train operators need to strengthen their network security design.

Remote access security

Remote access is used to give a trusted user or vendor access to the control system or network from a remote location. If not properly secured, remote access can provide a 'back door' entry for a hostile actor into the control system or network.

Our vulnerability assessment showed that train operators need to strengthen the security of their remote access.

Legacy operating systems

Periodic patching is aimed at improving the overall security of systems by reducing the number of vulnerabilities and the likelihood of exploitation.

Our vulnerability assessment showed that train operators need to strengthen their periodic patching of operating systems and applications within their control system environment.

3.4 Addressing cyber security vulnerabilities

During this audit, the Acting Auditor-General issued management letters to PTV outlining the findings of our assessment against the cyber security framework and our assessment of control system vulnerabilities. We sought assurance that consequent risks had been identified and assessed and, where necessary, that risk management processes have been put in place. The Acting Auditor-General asked PTV to work with train operators to identify remediation actions and specified time frames for these actions. PTV responded, outlining its intended actions and time frames.

We will periodically examine whether these findings are being addressed within an acceptable time frame. At our discretion, we may report to Parliament on PTV's progress.

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 Economic Development, Jobs, Transport & Resources, the Department of Justice and Regulation, Emergency Management Victoria, Public Transport Victoria, Victorian Rail Track and V/Line Proprietary Limited for submissions and comments.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

RESPONSE provided by the Secretary, Department of Economic Development, Jobs, Transport & Resources

Department of Economic Development,
Jobs, Transport and Resources

GPO Box 4509
Melbourne Victoria 3001 Australia
Telephone: 03 9651 9999
www.economicdevelopment.vic.gov.au
DX 210074

Ref: DOC/16/419733

RECEIVED
21 OCT 2016
VICTORIAN AUDITOR-GENERAL'S OFFICE

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 24, 35 Collins Street
MELBOURNE VICTORIA 3000

Dear Mr Greaves

Performance Audit Report *Security of Critical Infrastructure Control Systems for Trains*

Thank you for your letter of 5 October 2016 enclosing the performance audit report on the *Security of Critical Infrastructure Control Systems for Trains.*

I accept the recommendation that the Department of Economic Development, Jobs, Transport & Resources establish appropriate processes to manage the transfer of accountability and responsibility for audit recommendations.

I welcome the work Public Transport Victoria (PTV) has commenced in developing governance arrangements, systems and processes that aim to address the findings and recommendations, including working closely with train operators to implement improvements to ensure safer and more reliable control systems.

The Department is committed to ensuring the security of critical infrastructure control systems and will support PTV to implement the report's recommendations.

Yours sincerely

Richard Bolt
Secretary
21/10/16

VICTORIA
State Government

RESPONSE provided by the Secretary, Department of Justice & Regulation

Department of Justice and Regulation

Secretary

121 Exhibition Street
Melbourne Victoria 3000
GPO Box 4356
Melbourne Victoria 3001
Telephone: (03) 8684 0500
Facsimile: (03) 8684 0525
greg.wilson@justice.vic.gov.au
justice.vic.gov.au
DX: 210220

19 OCT 2016

Our ref: CD/16/504836

Mr Andrew Greaves
Auditor General
Victorian Auditor-General's Office
Level 24, 35 Collins Street
MELBOURNE VIC 3000

Dear Mr Greaves

Proposed Report Security of Critical Infrastructure Control Systems for Trains

Thank you for your letter of 6 October 2016 regarding the Proposed Report (the report) for the *Security of Critical Infrastructure Control Systems for Trains* audit, and the invitation to provide a formal response.

The Department of Justice and Regulation recognises the importance of the security of critical ICT management systems and notes the findings in the report.

Thank you providing the opportunity to provide comment on the report.

Yours sincerely

Greg Wilson
Secretary

RESPONSE provided by the Chief Executive Officer, Public Transport Victoria

PUBLIC TRANSPORT VICTORIA

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 24, 35 Collins Street
MELBOURNE VIC 3000

PO Box 4724
Melbourne Victoria 3001
Australia
Telephone 1800 800 007
ptv.vic.gov.au

Dear Mr Greaves

Proposed Performance Audit Report *Security of Critical Infrastructure Control Systems for Trains*

Thank you for your letter of 5 October 2016 inviting a response to the proposed performance audit report *Security of Critical Infrastructure Control Systems for Trains*.

Public Transport Victoria (PTV) has reviewed the report and accepts its recommendations. PTV is fully aware that the security of critical infrastructure control systems is of paramount importance and is absolutely committed to ensuring operators are aware of their responsibilities and have action plans in place. These plans will be rigorously monitored and audited.

PTV also understands the increasing threat to IT systems from automated and sophisticated cyber attacks and has since 2014, employed a dedicated IT security resource to implement security risk frameworks and controls in line with government standards and industry requirements. This resource will continue to mitigate the risk and work closely with industry bodies and experts, other agencies, and the operators to implement standards and controls that can reduce the threat and impact of cyber attacks.

PTV has also established an executive Information Security Steering Committee to oversee the implementation of a public transport wide governance structure, and defined a policy deployment and assurance framework, detailing the responsibilities for cyber security of control systems, that is currently being implemented.

PTV and operators have identified an executive director who will be directly accountable for information security in ICT and OCS within their organisation.

As identified in the report there will need to be significant future funding and resources to address this issue and update systems across the network. This has been recognised in the requirements in the renegotiating of the franchise contracts with rail operators. These negotiations will take place during early 2017.

Thank you for the opportunity to comment on the report.

Yours sincerely

Jeroen Weimar
Chief Executive Officer
20/10/2016

Page 1 of 3

RESPONSE provided by the Chief Executive Officer, Public Transport Victoria – continued

Attachment 1: Action Plan

	Recommendation	Proposed Action	Completion Date
1	Formalise governance arrangements with train operators and determine responsibilities for the cyber security of control systems	PTV accepts the recommendation. PTV has established an executive Information Security Steering Committee to oversee the implementation of a public transport wide governance structure., and defined a policy deployment and assurance framework, detailing the responsibilities for cyber security of control systems, that is currently being implemented. All operators have been recently reminded of their responsibilities for cyber security in writing. PTV's responsibilities have also been clearly documented and discussed with operators. PTV and operators have recently appointed an executive director who will be accountable for information security in ICT and OCS within their organisation.	31/12/2016
2	Prepare a cyber security strategy for control systems that establishes: • the desired level of security • governance arrangements that ensure adequate oversight.	PTV accepts the recommendation. PTV is establishing an "Information Security Working Group" with representatives from PTV, VicTrack and each operator, to carry out public transport wide risk profile assessments and to draft a strategic plan for endorsement by PTV's "Information Security Steering Committee", which includes the desired level of security per asset category and governance arrangements that ensures adequate oversight.	31/05/2017
3	Include in the renegotiated franchise and service agreements with train operators: • a clarification of ownership, roles and responsibilities for the management and operation of control systems • requirements for the management of control system security.	PTV accepts the recommendation. PTV has drafted a cyber security clause in consultation with the Australian Signals Directorate, the Office of the Commissioner for Privacy and Data Protection and the Information Security Advisory Group of the Victorian Government for inclusion in the renegotiated franchise contract. The new cyber security clause clearly defines ownership, roles and responsibilities as well as minimum requirements for the management of control system security.	30/11/2016
4	Establish funding arrangements for control system upgrades, renewals and maintenance as part of the renegotiation of franchise and service agreements	PTV accepts the recommendation. The funding arrangements for control systems has been included in the renegotiation of the new franchise contracts	30/11/2016
5	Identify and appoint a team of suitably qualified and experienced professionals to provide advice to the train operators on security, risk and business continuity management	PTV accepts the recommendation. PTV has appointed an Information Security Manager with responsibility to establish a virtual team with nominated subject matter experts from PTV, VicTrack and each operator to determine requirements and to provide advice to the train operators on security, risk and business continuity management.	31/10/2016
6	Establish appropriate processes for accountability, tracking, management and reporting of their actions and train operators' actions, in response to audit recommendations	PTV accepts the recommendation. PTV has commenced a program to: - define a governance and management structure for effective implementation of and reporting on corrective actions - assign accountability for Information & Controls Security to nominated executive directors of each organisation - establish "PTV Information & Controls Security Steering Committee" for tracking implementation of audit recommendations including regular reviews against action plans - establish "Information & Controls Security Working Group" for coordinating the management of, and reporting on, corrective actions - establish a program office in the CIO division to consolidate, coordinate and track operators activities in response to the VAGO audit - conduct another review of overall control systems in the 12 months	15/12/2016

RESPONSE provided by the Chief Executive Officer, Public Transport Victoria – continued

	Recommendation	Proposed Action	Completion Date
7	Advise train operators on how to implement appropriate risk management systems that identify, measure and monitor control system risks, by: • setting up a risk register • performing a risk analysis of identified security vulnerabilities to determine whether to immediately introduce security controls and/or technical fixes • applying the Victorian Government Risk Management Framework to consider inter-agency and relevant state significant risks.	PTV accepts the recommendation. PTV has defined a risk management approach, based on the Victorian Risk Management Framework, ISO27005 and industry best practices, that is currently being rolled out to operators. This includes updating risk registers and categorising risks into: - Risks that are common and/or for which there is an established treatment by implementing controls recommended by standards (e.g. CIS, ASD ISM, PSPF) - Risks for which no appropriate standard controls exist, that are unusual or potentially serious; these risks require more detailed assessment and customised treatment. The register will include relevant state and interagency significant risks. Organisation have been advised in writing, guidance is provided by the "Information Security Working Group" and effectiveness is monitored by the "Information Security Steering Committee"	30/11/2016
8	Advise train operators on how to implement appropriate compliance management systems that include: • processes to monitor, measure, evaluate and report on the performance of security controls • internal audit programs to regularly carry out vulnerability assessments or security tests to validate train operators' control system security.	PTV accepts the recommendation. PTV is implementing an "Information & Controls Security Working Group" to define and deploy public transport wide processes for 1. performing a risk profile assessment, and 2. definition of a "Protective Data Security Plan", which sets out the processes to monitor, measure, evaluate and report on the performance of security controls 3. coordinating internal audit and assessment programs	30/06/2017
9	Set up a security controls framework that aims to identify, detect, prevent and respond to cyber threats and that: • clearly defines minimum requirements and key performance indicators • references the Victorian Protective Data Security Framework, Victorian Protective Data Security Standards and the security architecture that train operators should use for their respective control system environments • includes requirements for monitoring and reporting security incidents • includes a schedule of audits that Public Transport Victoria will carry out, to monitor how the security controls framework is applied and managed • requires staff training in security for control systems • includes guidelines for sharing information with train operators to improve the security of control systems.	PTV accepts the recommendation. PTV has commenced the implementation of a public transport wide "Protective Data Security Plan" according to the Victorian Protective Data Security Framework, which includes - security capabilities to identify, detect, prevent and respond to cyber threats and processes according to Australian Signals Directorate's "Strategies to Mitigate Targeted Cyber Intrusions" - processes to clearly identify minimum requirements and KPI's - an approved "Information Security Management System" per organisation that defines standard security controls, employee training requirements, processes for security monitoring and response, assurance processes, etc. according to the Australian Signals Directorate's "Information Security Manual" The framework will include guidelines for sharing information and a regular audit program.	31/03/2018

RESPONSE provided by the Chief Executive Officer, V/Line Proprietary Limited

V/Line Pty Ltd Level 9, 750 Collins Street, Docklands, VIC 3008. GPO Box 5343, Melbourne VIC 3001. T (03) 9619 5900 F (03) 9619 5000
vline.com.au

20 October 2016

Mr Andrew Greaves
Auditor – General
Victorian Auditor – General's Office
Level 24, 35 Collins Street
Melbourne VIC 3000

Dear Mr Greaves

Re: Proposed Performance Audit Report – Security of Critical Infrastructure Control Systems for Trains

Thank you for your letter dated 5 October 2016 enclosing the proposed Performance Audit Report on the Security of Critical Infrastructure Control Systems for Trains and the opportunity to provide comment in accordance with section16(3) of the *Audit Act 1994*.

V/Line Pty Ltd (V/Line) notes the findings raised in the audit report and will work with Public Transport Victoria in ensuring that the recommendations are delivered in accordance with the agreed timeframes. V/Line will work closely with Public Transport Victoria to ensure that the risks to the delivery of essential passenger train services are managed appropriately.

Should you require any further information, please contact Phil Beale, Chief Financial Officer, V/Line Pty Ltd, on 03 9619 5939 or by email at phil.beale@vline.com.au.

Thank you again for the opportunity to provide comment.

Yours sincerely

Gary Liddle
Chief Executive Officer

V/Line Pty Ltd ABN 29 087 425 269

Auditor-General's reports

Reports tabled during 2016–17

Report title	Date tabled
Enhancing Food and Fibre Productivity (2016–17:1)	August 2016
Audit Committee Governance (2016–17:2)	August 2016
Meeting Obligations to Protect Ramsar Wetlands (2016–17:3)	September 2016
Efficiency and Effectiveness of Hospital Services: Emergency Care (2016–17:4)	October 2016
High Value High Risk 2016–17: Delivering HVHR Projects (2016–17:5)	October 2016

VAGO's website at www.audit.vic.gov.au contains a comprehensive list of all reports issued by VAGO.

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

Availability of reports

All reports are available for download in PDF and HTML format on our website www.audit.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