Appendices

Appendix 1: About the audit

This audit assessed whether the systems used to operate and manage critical infrastructure are secure and if systems go down, there are sound recovery arrangements.

Audit scope

Process control systems are widely used in utilities, transport and other infrastructure. We propose to focus on water and sewer supply and metropolitan traffic management.

We have focused on water and sewerage systems due to the potential:
- impact on supply and the health and safety consequences thereof
- physical damage to plant and equipment that can be caused by a hack on a water/sewage control system (for example broken valves, burnt-out pumps etc).

We have focused on metropolitan traffic management because of:
- the sensitivity of Sydney road systems to any disruptions, with the consequence of major congestion
- the safety risk associated with traffic management failures, including failed traffic lights
- a recent Queensland Audit Office audit on the security of traffic management systems found significant weaknesses.

The audit did not examine:
- efficiency and effectiveness of the selected process control systems in undertaking their functions of traffic control and water/wastewater management, except regarding the effectiveness of security and business continuity planning and management
- efficiency and effectiveness of other IT management systems implemented across the organisations, nor the IT security or business continuity arrangements in the organisations generally.

While the audit expressed an opinion on security and business continuity arrangements for the selected systems, it is not intended to identify all issues or potential issues in these systems or their wider environment. The audit was undertaken on a risk basis having regard to the resources and time available for the audit. The audit does not guarantee the security of the audited systems or that business continuity would be efficiently and effectively achieved in the event of an incident. It can only comment on the risks and mitigation of these risks.

Details of our approach to selecting topics and our forward program are available on our website.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standards ASAE 3500 on performance auditing, and to reflect current thinking on performance auditing practices. Our processes have also been designed to comply with the auditing requirements specified in the Public Finance and Audit Act 1983.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by the RMS, SWC and TfNSW. In particular we wish to thank our liaison officers and staff who participated in interviews and provided material relevant to the audit.
Audit team
Gary Gaskell and Neil Avery conducted the performance audit. Sean Crumlin and Kathrina Lo provided direction and quality assurance.

Audit cost
Including staff costs, printing costs and overheads, the estimated cost of the audit is $247,969.
Appendix 2: Glossary of terms

An **Access Control List (ACL)**, with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are granted on written objects. For instance, an ACL might give Alice access to read and write a file and Bob access to only read it.

In computer security, a **DMZ** or demilitarised zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organisation's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.

A **Disaster Recovery Plan (DRP)** is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Given organisations' increasing dependency on information technology to run their operations, a disaster recovery plan is increasingly associated with the recovery of information technology data, assets, and facilities.

An **Information Security Management System (ISMS)** is a management process with a set of policies concerned with information security management or IT related security and availability risks. The governing principle behind an ISMS is that an organisation should implement, design and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

An **Intrusion Detection System (IDS)** is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

A **Local Area Network (LAN)** is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building, using network media. The defining characteristics of LANs, in contrast to wide area networks (WANS), include their smaller geographical area and non-inclusion of leased telecommunication lines.

**Logical security** consists of software safeguards for an organisation's systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorised users are able to perform actions or access information in a network or workstation. It is a subset of computer security.

A **security zone** is an area within a network occupied by a group of systems and components with similar requirements for the protection of information and characteristics associated with those requirements. These shared requirements and characteristics will include a common data classification, including shared:

- data confidentiality and integrity requirements
- access controls
- audit, logging, and monitoring requirements.

A **Server** is a running instance of an application (Software) capable of accepting requests from the client and giving responses accordingly. Servers can run on any computer including dedicated computers, which individually are also often referred to as ‘the server’. In many cases, a computer can provide several services and have several servers running. The advantage of running servers on a dedicated computer is security.

Servers often provide essential services across a network, either to private users inside a large organisation or to public users via the Internet. Typical computing servers are database servers, file servers, mail servers, print servers, web servers, gaming servers, and application servers.
**Standard Operating Environment** (SOE) is a standard implementation of an operating system and its associated software. SOEs can include the base operating system, a custom configuration, standard applications used within an organisation, software updates and service packs. An SOE can apply to servers, desktops, laptops and mobile devices.

**Virtual Private Network** (VPN) extends a private network across a public network, such as the internet. It enables a computer to send and receive data across shared or public network as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

A **Workstation** is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems. The term workstation has also been used loosely to refer to everything from a mainframe computer terminal to a PC connected to a network.

A **business continuity plan** is a plan to continue operations if a place of business (for example, an office, worksite or data center) is affected by adverse physical conditions, such as a storm, fire or crime. Such a plan typically explains how the business would recover its operations or move operations to another location. For example, if a fire destroys an office building or data center, the people and business or data center operations would relocate to a recovery site.
Appendix 3: Key Recommendations from the TISN Critical Infrastructure Security Guidelines

Australian Government/Industry Trusted Information Sharing Network for Critical Infrastructure Resilience for Systems of National Significance developed by the IT Security Expert Advisory Group (ITSEAG) of the Critical Infrastructure Advisory Council (CIAC). Below are some extracts from the security guidelines that provide example of the TISN’s recommendations for the securing of SCADA or operational technology.

Generic SCADA Risk Management Framework for Australian Critical Infrastructure

- Where organisations have existing Corporate Risk Management and Security Frameworks in place it is important that this SCADA risk framework aligns with the corporate frameworks to ensure organisational consistency.
- Risks associated with external interdependencies such as an incident impacting multiple organisations (for instance with supply chains and business partners) should be considered.
- The risk management scope should include:
  - centralised SCADA Management and Control
  - data communications
  - front-end processing
  - field monitoring and control.

SCADA Architecture Principles – Good Practice Guide

- Detailed security architecture and zone requirements are documented in SCADA design specifications.
- The SCADA zone is not accessible from untrusted or semi-trusted networks.
- Good practice: Connections in and out of the SCADA zone are kept to a minimum
- Best practice: Controls should be in place at the internal DMZ that limits any interaction originating from the IT environment to the internal DMZ (or operational technology/SCADA environment).
- Users in the IT environment cannot perform actions in the operational technology (SCADA) environment.
- Security testing occurs annually or whenever changes to the architecture occur.

Implementing Gateways – Good Practice Guide

- Gateway security zones are separated through the use of appropriately configured firewalls.
- Appropriate logging and monitoring procedures are performed at gateway devices.
- Potential vulnerabilities are monitored through review of security bulletins and subscription services where available.
- Signature based intrusion detection systems maintain an up to date list of attack signatures.
- Alerts are monitored 24 hours a day. Any alerts are reviewed as a security incident and tuned on an ongoing basis.
- Incident response procedures are in place.
- Best Practice:
  - A security information and event management (SIEM) solution is in place for centralised log management.
  - Network controls restrict access on physically dedicated communication links.
Hardening of SCADA ICT Systems Good Practice Guide

- Segregate the SCADA network from the corporate network utilising a DMZ and stateful firewall.
- Ensure critical components provide required redundancy.
- Ensure only authorised personnel can access or operate SCADA system.
- Configure systems to prompt users to change passwords prior to an expiry date being reached.
- Ensure unique user IDs are assigned to all users.
- Ensure that generic logins are not used to authenticate into administrative consoles.
- Enforce the construction of strong passwords within SCADA systems.
- Ensure that the latest service packs and critical (software) patches are applied to servers.
- Ensure that the latest vendor approved firmware, patches and critical updates are applied to field devices.
- Implement anti-virus gateways to monitor outgoing and incoming web and email traffic.
- Encrypt information transmitted over wireless networks.
- Develop and conduct a programme to perform vulnerability assessments and penetration tests.
- Develop and maintain a business continuity management process.
- Best practice:
  - Implement an account lock-out counter
  - Prohibit the use of external media where possible.

Monitoring of SCADA Networks – Good Practice Guide

- Implement network intrusion detection on the SCADA network.
- Unauthorised parties should not be able to alter log source processes, executable files, configuration files, or other components.
- Utilise anti-virus detection software on all servers and workstations within the SCADA network.
- Implement a centralised real-time monitoring platform.

SCADA Good Practice Guide – Knowing Your Network

- SCADA roles and responsibilities are clearly defined.
- Risk assessments are performed over SCADA networks.
- Training and security awareness procedures are in place for SCADA personnel.
- Vulnerability management policies and procedures are in place.
Performance auditing

What are performance audits?
Performance audits determine whether an agency is carrying out its activities effectively, and doing so economically and efficiently and in compliance with all relevant laws.

The activities examined by a performance audit may include a government program, all or part of a government agency or consider particular issues which affect the whole public sector. They cannot question the merits of government policy objectives.

The Auditor-General’s mandate to undertake performance audits is set out in the Public Finance and Audit Act 1983.

Why do we conduct performance audits?
Performance audits provide independent assurance to parliament and the public.

Through their recommendations, performance audits seek to improve the efficiency and effectiveness of government agencies so that the community receives value for money from government services.

Performance audits also focus on assisting accountability processes by holding managers to account for agency performance.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, the public, agencies and Audit Office research.

What happens during the phases of a performance audit?
Performance audits have three key phases: planning, fieldwork and report writing. They can take up to nine months to complete, depending on the audit’s scope.

During the planning phase the audit team develops an understanding of agency activities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the agency or program activities are assessed. Criteria may be based on best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork the audit team meets with agency management to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with agency management to check that facts presented in the draft report are accurate and that recommendations are practical and appropriate.

A final report is then provided to the CEO for comment. The relevant minister and the Treasurer are also provided with a copy of the final report. The report tabled in parliament includes a response from the CEO on the report’s conclusion and recommendations. In multiple agency performance audits there may be responses from more than one agency or from a nominated coordinating agency.

Do we check to see if recommendations have been implemented?
Following the tabling of the report in parliament, agencies are requested to advise the Audit Office on action taken, or proposed, against each of the report’s recommendations. It is usual for agency audit committees to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament’s Public Accounts Committee (PAC) to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report is tabled. These reports are available on the parliamentary website.

Who audits the auditors?
Our performance audits are subject to internal and external quality reviews against relevant Australian and international standards.

Internal quality control review of each audit ensures compliance with Australian assurance standards. Periodic review by other Audit Offices tests our activities against best practice.

The PAC is also responsible for overseeing the performance of the Audit Office and conducts a review of our operations every four years. The review’s report is tabled in parliament and available on its website.

Who pays for performance audits?
No fee is charged for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports
For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.
<table>
<thead>
<tr>
<th>No</th>
<th>Agency or issues examined</th>
<th>Title of performance audit report or publication</th>
<th>Date tabled in parliament or published</th>
</tr>
</thead>
<tbody>
<tr>
<td>247</td>
<td>Roads and Maritime Services WestConnex Delivery Authority Infrastructure NSW Transport for NSW NSW Treasury Department of Premier and Cabinet</td>
<td>WestConnex: Assurance to the Government</td>
<td>18 December 2014</td>
</tr>
<tr>
<td>246</td>
<td>Department of Education and Communities</td>
<td>The Learning Management and Business Reform Program</td>
<td>17 December 2014</td>
</tr>
<tr>
<td>245</td>
<td>Environment Protection Authority Department of Trade and Investment, Regional Infrastructure and Services</td>
<td>Managing contaminated sites</td>
<td>10 July 2014</td>
</tr>
<tr>
<td>244</td>
<td>Office of Finance and Services Department of Education and Communities Forestry Corporation of NSW Fire and Rescue NSW NSW Businesslink Pty Ltd Essential Energy Sydney Trains</td>
<td>Making the most of Government purchasing power – Telecommunications</td>
<td>26 June 2014</td>
</tr>
<tr>
<td>243</td>
<td>NSW Treasury</td>
<td>Use of purchasing cards and electronic payment methods</td>
<td>5 June 2014</td>
</tr>
<tr>
<td>242</td>
<td>NSW Police Force</td>
<td>Effectiveness of the new Death and Disability Scheme</td>
<td>22 May 2014</td>
</tr>
<tr>
<td>241</td>
<td>Road and Maritime Services</td>
<td>Regional Road funding – Block Grant and REPAIR programs</td>
<td>8 May 2014</td>
</tr>
<tr>
<td>240</td>
<td>NSW State Emergency Service</td>
<td>Management of volunteers</td>
<td>15 April 2014</td>
</tr>
<tr>
<td>239</td>
<td>Fire and Rescue NSW NSW Rural Fire Service</td>
<td>Fitness of firefighters</td>
<td>1 April 2014</td>
</tr>
<tr>
<td>238</td>
<td>Transport for NSW Department of Attorney General and Justice</td>
<td>Improving legal and safe driving among Aboriginal people</td>
<td>19 December 2013</td>
</tr>
<tr>
<td>237</td>
<td>Department of Education and Communities</td>
<td>Management of casual teachers</td>
<td>3 October 2013</td>
</tr>
<tr>
<td>236</td>
<td>Department of Premier and Cabinet Ministry of Health – Cancer Institute NSW Transport for NSW – Rail Corporation NSW</td>
<td>Government Advertising 2012-13</td>
<td>23 September 2013</td>
</tr>
<tr>
<td>235</td>
<td>NSW Treasury NSW Police Force NSW Ministry of Health Department of Premier and Cabinet Department of Attorney General and Justice</td>
<td>Cost of alcohol abuse to the NSW Government</td>
<td>6 August 2013</td>
</tr>
<tr>
<td>234</td>
<td>Housing NSW NSW Land and Housing Corporation</td>
<td>Making the best use of public housing</td>
<td>30 July 2013</td>
</tr>
<tr>
<td>233</td>
<td>Ambulance Service of NSW NSW Ministry of Health</td>
<td>Reducing ambulance turnaround time at hospitals</td>
<td>24 July 2013</td>
</tr>
<tr>
<td>No</td>
<td>Agency or issues examined</td>
<td>Title of performance audit report or publication</td>
<td>Date tabled in parliament or published</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>232</td>
<td>NSW Health</td>
<td>Managing operating theatre efficiency for elective surgery</td>
<td>17 July 2013</td>
</tr>
<tr>
<td>231</td>
<td>Ministry of Health&lt;br&gt;NSW Treasury&lt;br&gt;NSW Office of Environment and Heritage</td>
<td>Building energy use in NSW public hospitals</td>
<td>4 June 2013</td>
</tr>
<tr>
<td>230</td>
<td>Office of Environment and Heritage - National Parks and Wildlife Service</td>
<td>Management of historic heritage in national parks and reserves</td>
<td>29 May 2013</td>
</tr>
<tr>
<td>229</td>
<td>Department of Trade and Investment, Regional Infrastructure and Services – Office of Liquor, Gaming and Racing Independent Liquor and Gaming Authority</td>
<td>Management of the ClubGRANTS scheme</td>
<td>2 May 2013</td>
</tr>
<tr>
<td>228</td>
<td>Department of Planning and Infrastructure&lt;br&gt;Environment Protection Authority&lt;br&gt;Transport for NSW WorkCover Authority</td>
<td>Managing gifts and benefits</td>
<td>27 March 2013</td>
</tr>
<tr>
<td>227</td>
<td>NSW Police Force</td>
<td>Managing drug exhibits and other high profile goods</td>
<td>28 February 2013</td>
</tr>
<tr>
<td>226</td>
<td>Department of Education and Communities</td>
<td>Impact of the raised school leaving age</td>
<td>1 November 2012</td>
</tr>
<tr>
<td>225</td>
<td>Department of Premier and Cabinet Division of Local Government</td>
<td>Monitoring Local Government</td>
<td>26 September 2012</td>
</tr>
<tr>
<td>224</td>
<td>Department of Education and Communities</td>
<td>Improving the literacy of Aboriginal students in NSW public schools</td>
<td>8 August 2012</td>
</tr>
<tr>
<td>223</td>
<td>Rail Corporation NSW Roads and Maritime Services</td>
<td>Managing overtime</td>
<td>20 June 2012</td>
</tr>
<tr>
<td>222</td>
<td>Department of Education and Communities</td>
<td>Physical activity in government primary schools</td>
<td>13 June 2012</td>
</tr>
<tr>
<td>221</td>
<td>Community Relations Commission For a multicultural NSW Department of Premier and Cabinet</td>
<td>Settling humanitarian entrants in NSW: services to permanent residents who come to NSW through the humanitarian migration stream</td>
<td>23 May 2012</td>
</tr>
<tr>
<td>220</td>
<td>Department of Finance and Services&lt;br&gt;NSW Ministry of Health&lt;br&gt;NSW Police Force</td>
<td>Managing IT Services Contracts</td>
<td>1 February 2012</td>
</tr>
</tbody>
</table>

Performance audits on our website

A list of performance audits tabled or published since March 1997, as well as those currently in progress, can be found on our website [www.audit.nsw.gov.au](http://www.audit.nsw.gov.au).
The role of the Auditor-General

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the Public Finance and Audit Act 1983.

Our major responsibility is to conduct financial or ‘attest’ audits of State public sector agencies’ financial statements. We also audit the Total State Sector Accounts, a consolidation of all agencies’ accounts.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to agencies to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to agencies and reports periodically to parliament. In combination these reports give opinions on the truth and fairness of financial statements, and comment on agency compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an agency is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an agency’s operations, or consider particular issues across a number of agencies.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General’s Reports to Parliament—Financial Audits.

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38E of the Public Finance and Audit Act 1983, I present a report titled Fitness of firefighters: Fire and Rescue NSW and NSW Rural Fire Service.

Grant Hehir
Auditor-General
1 April 2014

Our vision
To make the people of New South Wales proud of the work we do.

Our mission
To perform high quality independent audits of government in New South Wales.

Our values
Purpose – we have an impact, are accountable, and work as a team.
People – we trust and respect others and have a balanced approach to work.
Professionalism – we are recognised for our independence and integrity and the value we deliver.
New South Wales Auditor-General’s Report
Performance Audit
Fitness of firefighters

Fire and Rescue NSW
NSW Rural Fire Service