Submission No 5

EXAMINATION OF THE AUDITOR-GENERAL'S PERFORMANCE AUDIT REPORTS DECEMBER 2014 - JUNE 2015

Organisation:	Sydney Water
Name:	Mr Kevin Young
Position:	Managing Director
Date Received:	22 March 2016

Sydney
WATER

22 March 2016

Mr Bruce Notley-Smith MP
Chair
Legislative Assembly
Public Accounts Committee
Parliament House
Macquarie Street
SYDNEY NSW 2001

Performance audit report – Security of Critical IT Infrastructure

Dear Mr Notley-Smith,

Sydney Water welcomed the NSW Auditor General’s performance audit of the security of our critical information technology systems. Sydney Water considers these operations to be extremely important to ensure safe, reliable products continue to be produced and supplied to customers within our area of operations.

As noted by the auditor, Sydney Water is well equipped to deal with the impact of security incidents. Developed and tested procedures exist for response to security incidents and major outages. Multiple redundancies are also in place to ensure security is maintained such as the operation of a 24/7 monitoring centre with back-up systems and processes for key facilities and control units.

The report provided 11 recommendations that were specific to Sydney Water and we have been working towards implementing these improvements. The status of each recommendation is provided in the attached appendix.

If you have any questions regarding this information, please contact Patrick Gallagher, Manager of Risk and Resilience on 8849 4431.

Yours sincerely

Kevin Young
Managing Director

Appendix 1 Sydney Water *Security of Critical IT Infrastructure* Performance Audit

Implementation of recommendations March 2016

	Recommendation	**Accepted or rejected**	**Actions to be taken**	**Date to be actioned**	**Status** (completed / on track / delayed) **Progress update comments**	**Responsibility** (Division)
1	Extend the corporate ISMS to oversee the security of the process control environment, including the management of operational level risks and controls [***Key recommendation***].	Accepted	Extend the existing Sydney Water ISMS to incorporate the entire process control environment.	July 2015	Completed - August 2015. ISMS has been extended to the process control environment and has been issued. An external audit was held in August 2015. No non-conformities were noted.	Information Technology
2	Develop a comprehensive security plan for the whole environment (building on SWC's SCADA security policy) [***Key recommendation***]	Accepted	Sydney Water to document a comprehensive security plan.	July 2015	Completed - March 2016. First release of Security Plan in place. The plan has been synchronised with the latest version of the ISMS and SCADA security policy. This document will be under regular review to ensure continual improvement.	Service Delivery
3	Document and undertake additional risk mitigation to reduce risks to acceptable levels, and clearly document what levels of risk can be tolerated [***Key recommendation***].	Agreed in principle	Sydney Water conducts extensive risk assessments in line with its Corporate Risk Management framework. Sydney Water will improve the documenting and reporting of operational risks and controls.	July 2015	Completed - August 2015. Risks have been identified, collated, assessed and validated, with relevant updates to the Information Security Policy made. Accepted by GM, Service Delivery in August 2015, as required by ISMS.	Service Delivery

Recommendation		Accepted or rejected	Actions to be taken	Date to be actioned	Status (completed / on track / delayed) Progress update comments	Responsibility (Division)
4	Obtain documentary evidence to indicate that the risks associated with the security of process control systems at Prospect Treatment Plant have been mitigated to acceptable levels [***Key recommendation***].	Rejected*	*Sydney Water disagreed with the implication that there is an issue with risk management processes used by our partners. However, Sydney Water will continue to work with our partner to ensure appropriate mitigation of identified risks.	July 2015	Completed - January 2016. Review meetings held with the Prospect plant operator and all other Build Own Operate plant operators. Evidence of current state was obtained by Sydney Water. A review of the security of process control systems has been conducted and identified improvements implemented.	Service Delivery
5	Introduce a formalised procedure and approach to assessment of security alerts and the recording of risk management decisions in response to these alerts. This should include assessing the commodity application and control system vendor software vulnerability notices and recording the risk management decisions.	Accepted	Improvements to be made to the assessment of security alerts including a documented procedure and recording of assessments conducted.	July 2015	Completed - December 2014. Procedure HSS0013 Vulnerability Alerts Interim HSS Procedure has been produced and implemented. All security alerts and assessments are recorded and actioned according to this procedure.	Service Delivery

Recommendation		**Accepted or rejected**	**Actions to be taken**	**Date to be actioned**	**Status** (completed / on track / delayed) **Progress update comments**	**Responsibility** (Division)
6	Improve logging of security related events.	Agreed in principle	Sydney Water to consider implementation based on impacts to system operations.	July 2015	Delayed – estimated completion date December 2016. Security Incident and Event Management (SIEM) monitoring of firewalls has been implemented and monthly reporting process is in place. Sydney Water captures logging of denied access but cannot capture logs of all allowed access. While improvements to logging have been made, status is delayed due to required procurement of replacement network devices scheduled for mid-2016 with implementation expected in late 2016.	Information Technology
7	Investigate closer alignment to the TISN Critical Infrastructure Resilience Good Practice guidelines to more effectively manage threats to the system.	Accepted	Analyse alignment to TISN Critical Infrastructure Resilience Good Practice Guidelines for management of threats to the system.	December 2015	Delayed – estimated completion date April 2016. Considerable work has been done to align the SCADA Security Policy to TISN Critical Infrastructure Resilience Good Practice Guidelines. In addition this policy is being aligned to the National Institute of Standards and Technology Cyber Security Framework and Australian Signals Directorate (ASD) top 35 mitigation guidelines.	Information Technology

Recommendation		**Accepted or rejected**	**Actions to be taken**	**Date to be actioned**	**Status** (completed / on track / delayed) **Progress update comments**	**Responsibility** (Division)
8	Implement the Top 4 ASD (Australian Signals Directorate) mitigation guidelines.	Accepted	Develop process for implementation of Top 4 ASD mitigation guidelines.	December 2015	Delayed – estimated completion date June 2016. Top four mitigation guidelines will be implemented as part of Windows 7 hardening and patching actions. This is expected to be delivered by June 2016. The delay to implementation is due to the large number of sites to be included in this roll out, as well as restricted access to some plants that are currently undergoing critical operational changes.	Information Technology
9	Consider implementing the ASD top 35 mitigations guidelines for the protection of process control engineering workstations and SCADA servers.	Agreed in principle	An assessment of the cost effectiveness of implementing the ASD top 35 mitigations guidelines will be undertaken. Implementation to be based on case by case basis with system functionality the determining factor.	December 2016	On Track. ASD Top 35 mitigations guidelines review completed and current progress is: • 16 guidelines implemented • seven guidelines in progress (complete by April 2016) • six guidelines partially implemented • six guidelines not yet commenced. A decision on the cost effectiveness of implementing the remaining 12 mitigations guidelines that have been partially or not yet commenced will be made by April 2016.	Information Technology

Recommendation		Accepted or rejected	Actions to be taken	Date to be actioned	**Status** (completed / on track / delayed) **Progress update comments**	**Responsibility** (Division)
10	Determine the appropriate controls to limit unauthorised access to computer accounts including SCADA application software and computer operating systems [***Key recommendation***].	Accepted	Agreement on appropriate access, procedure development and implementation process.	July 2015	Completed – August 2015. Procedure for SCADA User Access Management approved and released. Appropriate access has been agreed and implemented as part of the security-hardened workstation and server device images. Outcomes documented in a formal procedure and endorsed by GM, Service Delivery in August 2015.	Service Delivery
11	Enhance monitoring of SCADA security.	Accepted	Investigate technical solutions for the enhancement of monitoring of SCADA security.	December 2015	Delayed – expected completion April 2016. The investigation process is now complete and a technical solution has been designed. Implementation enabling event logging and integration into SIEM is expected to be completed in April 2016.	Information Technology