Appendix three – About the audit

Audit objective

This audit assessed how well cyber incidents are monitored and remedial advice is communicated in the NSW public sector.

Audit criteria

We addressed the audit objective with the following lines of inquiry:

1. Cyber security incidents are monitored efficiently and effectively
    a) Processes are in place for monitoring cyber incidents within and across agencies.
    b) Appropriate mechanisms are in place for agencies to report cyber incidents, including clear guidance on whom to report to
    c) Counter-intelligence on cyber incidents is shared between state and federal agencies, and the private sector.
2. Agencies receive timely and quality advice on cyber incidents and remedial action
    a) Incidents are assessed and a suitable response determined
    b) Agencies under threat are notified
    c) Advice on remedial action is provided from internal and/or external sources.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. Incidents that have taken place since July 2015
2. Interviews with relevant staff in DFSI and the case-study agencies
3. Interviews with Australian Government agencies involved in coordinating cyber security
4. Review of documents on the relevant policies and procedures for detecting, monitoring and communicated cyber-events.

This audit focused on the following three areas:

1. Monitoring and detection of cyber incidents
2. Reporting and communication about cyber incidents
3. The communication of advice on remedial action.

A cyber incident, for the purposes of this audit, is a past or ongoing intrusion, disruption, or other event that impairs the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. Cyber incidents include major events impacting other jurisdictions, even if they do not directly impact NSW public sector agencies or universities.

Audit exclusions

The audit did not:

- Conduct a technical analysis on the adequacy of processes agencies used to detect and respond to cyber incidents
- Examine the controls agencies use to prevent cyber security incidents
- Analyse the quality of technical advice provided to agencies
- Question the merits of government policy objectives.

Audit approach

Our procedures included:

1. Interviewing relevant staff involved in detecting cyber security incidents, reporting cyber security incidents and, sharing information about cyber security incidents in the agencies.

2. Examining
   a) Procedures and processes for detecting and responding to cyber security incidents
   b) Information on cyber incidents reported since July 2016
   c) Procedures for gathering and sharing counter-intelligence information including communications with other government agencies, NGOs and the private sector.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards and technical advice from an expert consultant.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standards ASAE 3500 on performance auditing. The Standard requires the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. 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 cooperation and assistance provided by the Department of Finance, Services and Innovation and all of the case study agencies. In particular, we wish to thank our liaison officers and staff who participated in interviews and provided material relevant to the audit.

We would also like to thank other stakeholders that spoke to us and provided material during the audit.

Audit cost

Including staff costs, travel and overheads, the estimated cost of the audit is $348,342.