



## Standing Committee on Justice and Community Safety

### **Inquiry into Annual and Financial Reports 2021-2022** **ANSWER TO QUESTION TAKEN ON NOTICE**

---

Asked by Mr Cain MLA on 8 November 2022: Mr Shane Rattenbury took on notice the following question(s):

Reference: Hansard [uncorrected] proof transcript 8 November, Page 122

In relation to:

**THE CHAIR:** Okay, thank you. Attorney, I note the ACT Auditor-General released a report, a report on data security in 2020. Now that may seem a while ago, but it is very relevant, which found that, and I quote, 'key mandatory requirements of the ACT government's ICT security policy were lacking', unquote. Attorney, what action had Legal Aid taken to implement the recommendations of this Auditor-General report issued in 2020?

**Mr Rattenbury:** Can I just clarify with you, Chair, I understand Legal Aid is appearing before this committee tomorrow morning, is that—are these matters that you want to take up directly with the Legal Aid Commission at that point in time? Because—

**THE CHAIR:** I certainly can.

**Mr Rattenbury:** Because we will end up, sort of, saying to you, we will have to take some of that on notice and we will have to go and ask Legal Aid, or you can ask them directly tomorrow morning. I am happy to be guided by your preference.

**THE CHAIR:** Legal Aid, yes they are colleagues tomorrow.

**MR BRADDOCK:** 8.55.

**THE CHAIR:** Right, thank you. Well, we are in your hands, Attorney, Legal Aid is appearing tomorrow.

**Mr Rattenbury:** Yes, so—

**THE CHAIR:** Do you have an answer to that question?

**Mr Rattenbury:** Sorry.

**THE CHAIR:** It may well be asked tomorrow as well.

**Mr Rattenbury:** As well, all right, well, in which case I will take the question on notice and seek advice from Legal Aid.

Shane Rattenbury MLA: The answer to the Member's question is as follows: –

Of the nine recommendations made in the Auditor General's 2020 report, the ACT Government agreed to six recommendations, partially agreed to one (5a) and agreed in principle to two (4d, 9). A copy of the Government Response can be found [here](#). A status update on those recommendations is provided below.

| Recommendation number and summary  | Status and action   |
|--|---|
| <p><b>Recommendation 1 – Agreed</b></p> <p><i>WHOLE OF GOVERNMENT DATA SECURITY RISK ASSESSMENT</i></p> <p>Shared Services (Chief Minister, Treasury and Economic Development Directorate) and the Security and Emergency Management Branch (Justice and Community Safety Directorate) should develop a whole-of-government data security risk assessment. The whole of government data security risk assessment should be reviewed and updated at scheduled intervals.</p>  | <p><b>Complete</b></p> <p>The Whole of Government Threat Risk Assessment (TRA) has been completed. The recommendations from the TRA have had priorities assigned and work is underway to address them.</p>  |
| <p><b>Recommendation 2 – Agreed</b></p> <p><i>ICT SECURITY POLICIES</i></p> <p>Shared Services (Chief Minister, Treasury and Economic Development Directorate) should:</p> <ul style="list-style-type: none"><li>a) revise and update the ICT Security Policy (August 2019) to accurately refer to supporting documents referred to in the policy. Where supporting documents and policies are out of date, they should be reviewed; and</li><li>b) develop policy guidance, in support of the ICT Security Policy, for ACT Government agencies on their responsibilities with respect to managing and monitoring ICT service vendors.</li></ul> | <p><b>Complete</b></p> <ul style="list-style-type: none"><li>a) The <a href="#">Cyber Security Policy</a> had a major revision in December 2020 and a further revision in February 2021 addressing this recommendation.</li><li>b) The Cyber Security Framework, consisting of the Cyber Security Policy and detailed complementary standards, are published on the Cyber Security Portal which is available and promoted to all Directorates. Comprehensive Cyber Security Responsibilities guidance is also published on the Cyber Security Portal to support System Owners and Managers in understanding their roles and responsibilities with managing and monitoring business systems and vendors. Specific guidance regarding recommended security requirements for cloud services has also been developed and published.</li></ul> |
| <p><b>Recommendation 3 – Agreed</b></p> <p><i>CYBERSEC CONTROLS AND REPORTING</i></p> <p>The Security and Emergency Management Branch (Justice and Community Safety</p>  | <p><b>In progress</b></p> <ul style="list-style-type: none"><li>a) The ACT Protective Security Framework (ACTPSF) is being revised in the context of the TRA (see above) and new</li></ul>  |

| Recommendation number and summary | Status and action |
|-----------------------------------|-------------------|
|-----------------------------------|-------------------|

Directorate), Shared Services (Chief Minister, Treasury and Economic Development Directorate) and the Office of the Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate), through the auspices of the Security and Emergency Management Senior Officials Group should:

- a) review and update the CYBERSEC requirements of the ACT Protective Security Policy Framework to reflect the most important system security measures from the ICT Security Policy (August 2019). These measures should be targeted at the areas of agency responsibility and able to be reported in dashboard form; and
- b) require agencies to report on the implementation of these measures in their ICT systems as part of the GOVSEC 4 reporting process of the ACT Protective Security Policy Framework, in order to provide reasonable assurance that data security risks are being effectively managed.

Commonwealth security of critical infrastructure legislation that regulates minimum standards of protective security for critical infrastructure entities, including government owned and operated critical infrastructure.

- b) The ACTPSF is being redeveloped to align more closely with the Commonwealth framework. This includes refining the governance security requirements and preparing clear standards that outline measures to meet. These measures will include reporting mechanisms and risk management. The new ACTPSF is due to be delivered by 30 June 2023, with implementation shortly thereafter.

**Recommendation 4 – Agreed /Agreed in Principle**

*DATA SECURITY STRATEGY*

The Office of the Chief Digital Officer and Shared Services (Chief Minister, Treasury and Economic Development Directorate) and Security and Emergency Management Branch (Justice and Community Safety Directorate), in partnership with ACT Government agencies, should document and agree a whole of government data security strategy and plan. This document should identify:

- a) The role and responsibilities of governance bodies and agencies responsible for managing and improving data security across ACT Government;
- b) Any related whole-of-government plans for addressing specific data security issues, such as the planned Cyber Security Incident Emergency Sub-plan to the ACT Emergency Plan;

**In progress**

- a) **Complete.** The ACT Data Governance and Management Policy Framework was endorsed and published in August 2020. It is being implemented by directorates (supported by CMTEDD and the Data Reform Group). Directors-General have appointed Executive Data Leads whose role will be to implement the Data Governance and Management Framework within Directorates. Whole of government oversight of its implementation is provided by the Data Reform Group and supported by the Data Management Group. Data-specific roles and responsibilities have been identified within directorates to ensure good data security practice.
- b) **Complete.** The Cyber Emergency Sub-Plan is in effect under the *ACT Emergency Plan*.
- c) **In progress.** A Cyber Security Essentials e-learning course has been developed for all staff, as well as a specific course designed for Executives. The training has been

| Recommendation number and summary  | Status and action  |
|--|--|
| <ul style="list-style-type: none"> <li>c) Activities and resources to improve data security for ACT Government; and</li> <li>d) Identifying the Chief Digital Officer as the responsible senior executive for implementing the strategy to improve data security across ACT Government.</li> </ul> | <p>available to staff on the Territory's WhoG learning management system.</p> <ul style="list-style-type: none"> <li>d) <b>Complete.</b> The Chief Digital Officer, together with the Data Reform Group and directorate Executive Data Leads is responsible for implementing the strategy to improve data governance and management, including protective security aspects across ACT Government.</li> </ul> |

**Recommendation 5 – Agreed / Partially agreed**

*SYSTEM SECURITY RISK MANAGEMENT PLAN ASSESSMENTS*

Shared Services (Chief Minister, Treasury and Economic Development Directorate) should:

- a) In conjunction with Recommendation 4, ensure agencies take account of the full cost of managing security across a system's lifecycle as part of ICT projects, including undertaking security assessments; and
- b) Address the backlog of security risk management plan assessments so that agencies can access security assessments and advice to help them manage data security risks in a timely manner.

- a) **Complete.** The 'Guiding Best Practice Design and Delivery' guide embeds security into the design and development of new and existing digital solutions, to ensure project sponsors and system owners make good design and investment decisions that reduce or mitigate security risks to provide a system that is safe and secure. Directorate Cyber Security reporting continues to be used to draw attention to security requirements for business systems and the need to resource and manage initial and ongoing security requirements.
- b) **In progress.** The backlog of security assessments has lessened but has not been resolved during this period. Funds provided in the 2021-22 budget for "Investing in public services: Strengthening cyber-security" have enabled additional staffing resources and software tooling to support more effective operations and service the increasing demand for security assessment services. The use of external security services for critical systems requiring assessment is also available.

**Recommendation 6 – Agreed**

*SYSTEM SECURITY MANAGEMENT PLANS*

The Security and Emergency Management Branch (Justice and Community Safety Directorate) and Shared Services (Chief Minister, Treasury and Economic Development Directorate) should:

- a) In conjunction with Recommendation 3, require ACT Government agencies to report on the currency of their system security risk management

**In progress**

- a) **Complete.** Digital Data and Technology Solutions (DDTS) continues to provide whole of government System Security Plan status information in the ICT Security report tabled at each Security and Emergency Management Senior Officials Group meeting. The Configuration Management Database (CMDB) is used as the common authoritative source of information about critical business systems.

| Recommendation number and summary   | Status and action  |
|---|--|
| <p>plans using a common authoritative list of critical systems; and</p> <p>b) In conjunction with Recommendation 1, develop a process to capture common risks and treatments from ACT Government agencies' system security risk management plans to inform the whole of government data security risk assessment.</p> | <p>b) <b>In progress.</b> Although the Whole of Government TRA has been finalised, the establishment of a centralised risk register for critical systems remains to be progressed.</p> |

**Recommendation 7 – Agreed**

*DATA SECURITY TRAINING*

Shared Services (Chief Minister, Treasury and Economic Development Directorate), with input from the Security and Emergency Management Branch (Justice and Community Safety Directorate) and the Office of the Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate), should coordinate the development of data security training that:

- a) Considers the specific training needs for all users, privileged users and executives; and
- b) addresses the risk of using unsanctioned methods of sharing sensitive personal data.

The data security training package should be capable of being delivered and customised by ACT Government agencies as necessary.

**In progress**

- a) **In progress.** A Cyber Security Essentials e-learning course has been developed for all staff, and a specific course designed for Executives has been completed. From October 2022, the training has been available on the HRIMS WhoG learning management system DDTS also provides cyber security awareness information through the Cyber Community of Practice and the Cyber Security Portal. These resources will continue to be complemented with cyber security awareness sessions delivered by DDTS to Directorates on an as needs basis.
- b) **Complete.** As per recommendation 4, the ACT Data Governance and Management Framework was endorsed by Strategic Board in August 2020.

**Recommendation 8 – Agreed**

*DATA BREACH RESPONSE PLANS*

The Security and Emergency Management Branch (JACS), the Office of the Chief Digital Officer and Shared Services (CMTEDD) should complete all agreed actions from the March 2019 Security and Emergency Management Senior Officials Group meeting to improve the data breach response processes.

**Complete**

The [Cyber Security Policy](#) provides a baseline requirement for agencies data breach plans to implement the policy.

The Data Reform Group have established an implementation plan for the Data Governance and Management Framework which will include the development of whole of Government guidance materials and templates relating to data breach policy and responses plans – as a way of supporting directorates to have consistent data security practices and governance within the Directorate's within their unique context and operating environment. A data breach plan for ACT's Whole of Government Data Lake is being finalised. This will be used as a foundation for other data breach plans across ACT Government.

**Recommendation number and summary****Status and action****Recommendation 9 – Agreed in principle****SYSTEM RESILIENCE PLANNING**

In conjunction with Recommendation 3, the Security and Emergency Management Branch (Justice and Community Safety Directorate), the Office of the Chief Digital Officer and Shared Services (Chief Minister, Treasury and Economic Development Directorate) should require ACT Government agencies to provide assurance through GOVSEC 4 reporting that appropriate levels of data recovery and system availability are in place for their critical ICT systems. The GOVSEC 4 reporting process could focus on the proportion of critical systems for which agencies have recently reviewed and tested their assurance in the event of the loss of availability of these systems.

**Complete**

DDTS have amended Security Risk Management Plans and processes to require critical systems owners to review the effectiveness of systems resilience and backup.

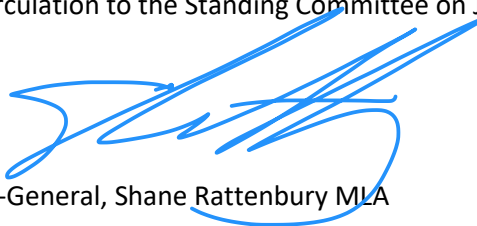
---

Legal Aid ACT is aware of the Auditor-General's report which focuses on the Government's Protective Security Policy Framework and ICT Security Policy.

The suite of ICT security measures in place at Legal Aid ACT were intended to meet the high general standards of the current threat environment.

Approved for circulation to the Standing Committee on Justice and Community Safety

Signature:



By the Attorney-General, Shane Rattenbury MLA

Date:

11/12/22