Supplementary Submission No 2a

EXAMINATION OF SELECTED AUDITOR-GENERAL'S FINANCIAL AUDIT REPORTS 2021

Organisation: Department of Customer Service

Date Received: 7 September 2022

NSW GOVERNMENT | Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
ABN 81 913 830 179 | www.nsw.gov.au

Office of the Secretary

Our reference: BN-05326-2022
Your reference: [redacted]

Greg Piper
Chair
NSW Public Accounts Committee
By email: PublicAccountsCommittee.PAC@parliament.nsw.gov.au

Dear Mr Piper

Follow up on Auditor-General's Financial Audit Report on Customer Service 2021

Thank you for your letter dated 17 August 2022 regarding a request to provide the Public Accounts Committee with an outline of action the Government has taken in relation to the recommendations in the report entitled *Financial Audit Report – Customer Service 2021,* tabled on 17 December 2021.

Please find attached the Department of Customer Service's response to the recommendations.

If you would like more information, please contact Lesley Honeyman, Acting NSW Chief Cyber Security Officer, via [redacted]

Yours sincerely

[redacted]

Emma Hogan
Secretary

Date: 06/09/22

August – Public Accounts Committee

1. **Did all required agencies submit these reports for the 2020-21 reporting period? If not:**

    1. **Which agencies met their reporting obligations?**

    All but two of the 194 eligible entities submitted their reporting for the 2020-2021 NSW Cyber Security Policy.

    2. **Which agencies have not met their reporting obligations, and which reporting obligations have not been met for each agency?**

    Two small entities that were a part of the Department of Primary Industry and Environment (DPIE – now Department of Planning and the Environment) Cluster.

    3. **For any pending reports, when are these expected to be received?**

    Repeated attempts at contacting the organisations through their Cluster Chief Information Security Officer (CISO) were unsuccessful. It is not expected they will provide reporting for that period.

2. **How does Cyber Security NSW assess the veracity of these reports? If an agency's report did not contain sufficient detail, would agencies be required to re-submit their reports?**

    Cyber Security NSW reviews all reporting data manually during collation and analysis. Reporting entities are regularly requested to provide more or clarifying information regarding their reporting. These are nearly always due to administrative errors or unclear comments within reporting and are not reflective of maturity issues.

Other

3. **How does Cyber Security NSW monitor agencies compliance with the NSW Cyber Security Policy? How does this inform Cyber Security NSW's programs to target/prioritise improvements to the NSW Government's cyber security resilience?**

    The NSW Cyber Security Policy is a risk-based policy. Compliance with the Policy means to have reported accurately, identifying a reporting entities areas of strength and weakness and identifying appropriate risks that could be caused by the entity's maturity level.

    Cyber Security NSW tracks reporting received and communicates directly with entities or their Cluster Chief Information Security Officer (CISO) where compliance concerns are raised.

    NSW Cyber Security Policy reporting data helps target and prioritise improvements in:

    - *Funding cases such as under the Digital Restart Fund*

- *Communicating to senior executives such as through the Secretaries Board*
- *Engagement from Cyber Security NSW through a variety of free services available to NSW Government entities.*

4. **What action does Cyber Security NSW or the Department take when agencies fail to meet the mandatory requirements of the NSW Cyber Security Policy?**

   As above, the NSW Cyber Security Policy is a risk-based policy. Compliance with the Policy means to have reported accurately and identifying appropriate risks that could be incurred by the entity's maturity level. If an agency reports a very low maturity level, this can inform engagement from Cyber Security NSW across the variety of free services on offer.

   A low maturity may indicate that they are not taking advantage of these services appropriately and linking the entity to these services can assist with lifting maturity for the following reporting period.

5. **How does Cyber Security NSW support agencies to meet the mandatory requirements of the NSW Cyber Security Policy?**

   Cyber security uplift against the NSW Cyber Security Policy is the responsibility of the reporting entity itself, but Cyber Security NSW provides clarification and assistance where possible. This includes:
   - *Extensive engagement on changes to the Policy and their impact on reporting entity maturity levels.*
   - *Assistance with Digital Restart Fund business cases to provide the required funding for uplift.*
   - *A variety of services that assist reporting entities meet certain maturity levels:*
     - *Cyber Security Awareness and Training*
     - *Incident response intelligence and operational assistance where required*
     - *Cyber security incident exercises*
     - *Cyber security "Health Checks"*
     - *Policy Guidance and templates*
   - *Monitoring of a Policy Mailbox which provides prompt and detailed advice for Government entities with queries about reporting against the Policy.*

Training and education activities

6. **How many public sector personnel did Cyber Security NSW provide training to in 2020-21 and 2021-22? Were personnel from each/all clusters in these training sessions?**

   NSW Government staff trained (both e-module and live):
   - *FY 2020-2021: 9,035*
   - *FY 2021-2022: 126,404*

7. **Please provide the June 2022 monthly uplift statistics for Cyber Security NSW's training program.**

    - *Live Training Completions: 345*
    - *Live Training Average Rating: 53 respondents rated 4.2 out of 5*
    - *E-module Completions: 23,494*
    - *E-module Average Rating:1569 respondents rated 8.5 out of 10*

8. **Has Cyber Security NSW assisted any agencies to develop their own internal cyber security training programs? If so, please provide details.**

    Cyber Security NSW have collaborated with clusters and agencies to tailor training content for their staff in live and e-module training. This includes developing e-module training and awareness materials for specific cohorts such as NSW Electoral Commission staff for the 2023 election, and tailoring e-module content (20 separate instances) for departments and agencies to ensure staff have locally specific cyber reporting instructions and links to contacts within their cluster. Cyber Security NSW have also co-hosted training sessions with clusters and agencies and developed awareness live sessions for targeted groups including Councillors and members of Parliament. In addition, there are currently 22 local councils using up to three instances of e-module training.

9. **What feedback has Cyber Security NSW received on its cyber security training programs and eModules? How has this feedback received informed Cyber Security NSW's future training programs.**

    Training feedback has been received on all sessions and e-module through post-session surveys, email feedback, e-module reviews and cluster engagement meetings. To date, over 70,000 reviews have been received. This data has been analysed for trends and reviewed on a regular basis to identify short and long-term changes for the training. During the tailored e-module development phase, Cyber Security NSW works closely with agencies or clusters to incorporate several rounds of feedback into the resulting e-module. Quizzes have also been conducted within live training to ascertain comprehension of cyber security awareness and Cyber Security NSW has consistently measured improvement in awareness across all learners.

10. **In the past 12 months how many cyber security exercises has Cyber Security NSW conducted?**

    Five exercises have been conducted. Two were large scale exercises (a whole-of-government exercise and an exercise for councils. Three were agency specific exercises.

Please provide examples of these exercises, including:

- **what sort of exercises were conducted**
    - *The exercises were discussion exercises.*
- **Whether any significant findings or recommendations were identified, and**
    - *Every exercise identifies recommendations. Predominantly, recommendations are made to improve specific aspects of an agency or council incident response plan.*

- **How have the exercises have improved cyber security resilience:**
    - *These exercises have aided in improving the NSW Government's cyber resiliency as they have allowed clusters, agencies and councils the ability to not only prepare for an inevitable cyber incident, but have provided organisations the ability to fully understand their roles and responsibilities during a cyber incident. Furthermore, Cyber Security NSW exercises have provided the NSW Government the ability to reduce the harm that may arise from an incident by providing the opportunity to test plans in a simulated environment, highlighting any weaknesses or gaps within those plans.*

Cyber security incidents

11. **How does Cyber Security NSW define what is a 'cyber security incident'? Is this a universal definition used across the NSW Government sector or does each agency use their own definition?'**

    The term 'cyber security incident' is defined in the NSW Government Incident Response Plan. All NSW Government agencies are required to report incidents falling within this definition to Cyber Security NSW under the NSW Cyber Security Policy. Agencies may have their own definitions or sub categories of incidents. This is not of concern as agencies have different risk postures and thresholds for what they may consider an incident. However, the whole of NSW Government definition provides the threshold for reportable incidents to Cyber Security NSW.

12. **How many cyber security incidents were reported to Cyber Security NSW in the financial reporting periods 2019-20, 2020-21 and 2021-22? Please provide the estimated financial impacts of these reported incidents for each financial reporting period.**

    The number, nature and impact of incidents, including those from state departments and or agencies who have been the subject to data breaches and/or hacking incidents, is not released for security reasons. Threat actors use this type of information for malicious purposes, including to further target NSW Government as knowing what we are detecting, monitoring and remediating allows them to tailor their attacks to optimise their success.

13. How many times was Cyber Security NSW involved in coordinating the NSW Government response to significant cyber security incidents and cyber crises in the financial reporting period 2019-20, 2020-21 and 2021-22?
    2019-20 – one
    2020-21 – one
    2021-22 – zero

14. **How does Cyber Security NSW use its experience from previous cyber security incidents to inform policies and programs to improve current cyber security resilience?**

    Cyber Security NSW uses these experiences to update the NSW Cyber Security Policy, the NSW Cyber Incident Response Plan and the NSW Cyber Security Incident Plan *which is a sub plan under the NSW Emergency Management Plan. Cyber Security NSW uses this information to provide actionable intelligence across the NSW Government sector to prevent and reduce the spread of incidents. Cyber Security NSW also uses this information to continuously improve awareness raising activities.*

Funding

15. **How many agencies have applied for cyber security uplift funding since the commencement of the Digital Restart Fund? Of those which applied, how many were successful?**

Forty-seven (47) business cases have been submitted to the Digital Restart Fund for cyber uplift. Some business cases cover entire clusters or multiple agencies within a cluster. All business cases are reviewed and subject to assurance upon submission and prior to receiving any approvals.

What types of cyber security uplift programs have successful applicants received funding for?

Agencies identify requirements to support the uplift of their cyber security maturity or to help reduce key cyber risks. This can include rolling out capabilities as part of implementing the Australian Cyber Security Centre (ACSC) Essential Eight and NSW Cyber Security Policy (For example; implementing security tools for application control).

16. **How are these funding applications prioritised, and how does the individual agency's current cyber security resilience factor into this assessment?**

The pipeline is prioritised around uplifting areas of low cyber security maturity against the NSW Cyber Security Policy and ACSC Essential Eight, as well as mitigating high and critical cyber security risks.

Overall NSW government cyber security resilience

17. **Across the NSW government sector, have any specific cyber security resilience areas been identified as requiring focused or priority uplift? If so, please outline:**
    - **How were these areas identified and by whom?**
    - **How are programmes and/or funding being updated to target improvement in these areas?**

Uplifting areas of low cyber security maturity (‘specific cyber security resilience areas’) has occurred regularly since receipt of maturity reporting data in August 2019. Areas of priority uplift vary. Annual reporting against the NSW Cyber Security Policy identifies areas of high and low maturity across government, and this data is referenced when providing whole-of-government and individual assistance to clusters and agencies. This information is also used in the development of cyber uplift business cases as part of the Digital Restart Fund process.

One example of prioritising cyber security uplift in the NSW Government is the *publication in 2020 of the DCS 2020-05 Cyber Security Directive that mandated mandatory cyber security training and cyber hygiene requirements for Agency/Department Executives and their staff. These uplift requirements were informed by maturity reporting.*

More generally, agencies and clusters tailor Digital Restart Fund uplift business cases to best mitigate existing and new high and critical cyber security risks, submitting new business cases as required to target improvement in critical areas or areas of low maturity.

18. In the past 12 months, how have policies, procedures and processes been improved to make Cyber Security NSW and NSW Government Agencies more effective in identifying, planning for and managing cyber security risks?

All policies and procedures in Cyber Security NSW are continually being improved based on customer feedback and analysis of best practice in other jurisdictions. In the past 12 months, the NSW Cyber Security Policy has incorporated several recommendations from NSW Audit Office reports and from an independent review of the Policy to strengthen Cyber Security NSW and NSW Government agencies' ability to identify, plan for and manage cyber security risks.

Recommendations already implemented include the reporting of target maturity levels, Agency head's acceptance of residual risk where target levels are low, the requirement to compile and retain in accessible form, the artefacts that demonstrate the basis for self-assessments and a process for agency heads charged with governance arrangements to formally accept residual cyber risks. Additional recommendations are being implemented in 2023 which is indicative of the continual improvement of the Policy and related policies and procedures.