
Appendix one – Response from agencies

Response from the Department of Premier and Cabinet



Ref: A3908166

Ms Margaret Crawford
Auditor-General for New South Wales
Level 19
Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000

RE: Special Audit – Compliance with the NSW Cyber Security Policy

Dear Ms Crawford

Thank you for the opportunity to provide a response to your draft report on the Special Audit – Compliance with NSW Cyber Security Policy (the **Report**).

I acknowledge your key findings and recommendations; my Department is implementing a Cyber Security Uplift Program which will address recommendations 4 and 5 for participating agencies.

I have major concerns about the Report being published in the public domain. The Report contains aggregated data on the current state of nine NSW Government Departments' cyber security maturity, including individual agencies' maturity against the Australian Cyber Security Centre's Essential 8.

Making this information available in the public domain would increase the risk of a successful cyber-attack against the nine NSW Government Departments covered by the Report.

I am also concerned that the Report has assessed that, to be compliant, an agency must reach level 3 maturity. This goes against the risk-based intent of the policy, which encourages agencies to identify the level of maturity that is appropriate for their organisation, given their risk profile.

In these circumstances, I respectfully request that the Audit Office consider options to allow:

- a public, summary version of the Report to be prepared for tabling in Parliament (containing, for example, only the Executive Summary of the Report); and
- a private, detailed version of the Report being made available for inspection by Members of Parliament on a confidential basis and to relevant agencies.

Yours sincerely

A handwritten signature in black ink, appearing to be 'TR'.

Tim Reardon
Secretary

14 July 2021

52 Martin Place, Sydney NSW 2000 ■ GPO Box 5341, SYDNEY NSW 2001
Tel: (02) 9228 5555 ■ www.dpc.nsw.gov.au

Response from the Department of Communities and Justice



Communities
& Justice

Margaret Crawford
Auditor-General for New South Wales
Audit Office of NSW
201 Sussex Street
SYDNEY NSW 2000

8 July 2021

Ref: EAP21/9556

Dear Ms Crawford

Special Audit – Compliance with the NSW Cyber Security Policy

Thank your letter dated 17 June 2021 and for the opportunity to respond to the recently completed audit.

DCJ considers the information in the report to be valuable for internal use.

Please find attached a table responding to each recommendation in the report. As you will see, we have outlined the action we will take in response to your recommendations about NSW Cyber Security policy.

The DCJ Chief Information Security Officer (CISO) recent met with the other departmental CISOs at the Cyber Security Senior Officers Group (CSSOG) meeting. There was consensus that the report provides an inappropriate amount of detail regarding the security maturity of departments.

Whilst it is appropriate to identify poor practice and behaviour, from a cyber-security perspective we ask that the Audit Office not be identify control weaknesses and publish them which may support a successful cyber-attack.

The approach taken by the Audit Office to publicly release this detailed information is out of step with industry standards and will assist attackers in better targeting agencies. Whilst other organisations undertake invasive audits and share their reporting with customers these reports are shared under a non-disclosure agreement and not released into the public domain.

An amended report focused on identifying over-inflated scoring (but not identifying the score) for departments should be developed. The report could identify non-compliance to the policy, but specific control references need to be removed.

I look forward to continuing our progress in relation to cyber security and compliance with the NSW Cyber Security policy including our response to the report's recommendations.

Should you require any further information please contact Thomas Thornton, Director, Audit, Risk and Compliance on 0475 985 672 or Thomas.Thornton@dcj.nsw.gov.au.

Yours sincerely

A handwritten signature in black ink, appearing to read 'M. Coutts-Trotter'.

Michael Coutts-Trotter
Secretary

Department of Communities and Justice
Postal address: Locked Bag 10, Strawberry Hills NSW 2012
W www.dcj.nsw.gov.au
T (02) 9377 6000 | TTY (02) 8270 2167
ABN 36 433 875 185

Response from the Department of Customer Service



Customer
Service

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

Office of the Secretary

Our reference: COR-06791-2021

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
By email: mail@audit.nsw.gov.au

A handwritten signature in black ink that reads 'Margaret'.

Dear Ms Crawford

Thank you for your letter dated 28 September 2021, and for the opportunity to respond to the *Compliance with the NSW Cyber Security Policy* final report (the Report). I would like to express gratitude to the Audit Office of New South Wales (NSW Audit Office) for its genuine engagement and consideration of concerns raised by the Department of Customer Service (the Department) regarding the sensitivity of information contained in previous iterations of the Report.

The Report raises important issues regarding the implementation of the NSW Cyber Security Policy (the Policy). As in previous NSW Audit Office reports, the analysis and recommendations play a critical role in improving cyber security resilience and the accountability of NSW Government entities.

I note that the Report examined the 2020 iteration of the Policy. The Policy has been updated since that time with version 4.0 released in April 2021. The Policy continues to undergo regular review and update. Cyber Security NSW has recently commissioned an independent external review of the Policy and is also consulting closely with State and Federal government agencies to identify potential changes. The Policy review will consider findings and recommendations from the NSW Audit Office and the Parliamentary Inquiry into Cybersecurity. This review and the feedback from ongoing consultation will enable the Policy to continue to evolve to address the changing technological and threat landscape as well as address lessons learnt.

The Department notes the recommendation to increase monitoring and compliance of maturity reporting to ensure greater accuracy. Cyber Security NSW's Governance, Risk and Compliance (GRC) team will be commencing a Maturity Assurance Review program with selected Policy mandatory requirements being reviewed across all Clusters. This program will assess the accuracy of maturity reporting, provide guidance for cyber security uplift requirements, and report uplift outcomes to Secretaries Board.

The Department notes the recommendations for agencies to report target maturity levels for each mandatory requirement and provide acceptance of residual risk for low target levels, and to better identify discrepancies in target maturity levels, risks associated with information held and services provided. These recommendations will be addressed in the review of the Policy.

The Department notes the recommendation to align the Policy closely to the Australian Cyber Security Centre's (ACSC) Essential Eight. Relevant sections of the 2022 NSW Cyber Security Policy will align with the recent updates to the Essential Eight framework.

The Department notes the concerns of the NSW Audit Office about the presence of a level 0 maturity for Essential Eight in the 2020 iteration of the Policy. However, the Department stands by its inclusion as part of supporting accurate assessment of maturity. This approach is supported by the re-introduction by the ACSC of level 0 in the July 2021 version of the

Essential Eight. This iteration of the Policy was made in consultation with the ACSC and industry partners. Cyber Security NSW would be happy to facilitate deeper engagement between the NSW Audit Office and the ACSC to ensure enhanced understanding of this framework and its implementation.

The Department notes the recommendation to prioritise improvements to cyber security and resilience across NSW Government agencies. The net decline in agency scores across the Policy in the 2020 reporting reflected a growing understanding by agencies on how to report maturity and Cyber Security NSW in analysing it. NSW Government is unique in its strategic view of uplift in cyber security and the Policy is a key element in achieving this. Agency uplift will be an ongoing journey that builds on learnings from all parties. A strong understanding of areas that require uplift help focus new iterations of the Policy and the engagement and assistance provided by Cyber Security NSW.

NSW Government is currently leading the nation by requiring its entities to assess and report on cyber maturity. To the best of our knowledge, no other State, Territory or Federal Government Department has the same strategic view of cyber security maturity which includes not only technical controls, but also people and process controls – or a detailed view of the status of whole-of-government cyber uplift.

The Department would like to highlight that this work is being supported through unprecedented levels of investment in cyber security. The NSW Government leads the nation with a \$240m investment dedicated to uplifting cyber maturity, with all clusters having started this process. This investment is part of \$1.6 billion over three years to ensure comprehensive digital transformation. This investment has been further supported by an additional \$500m injection to the Digital Restart Fund, which includes \$75m for cyber uplift in small agencies.

The NSW Government's dedication to the state's digital transformation journey, including in cyber security, has been reflected in recent benchmarks and indexing. This includes the NSW Government being ranked first (9.8/10) in the 2021 Intermedium Digital Government Readiness Indicator, and second (9.3/10) in the 2021 Intermedium Cyber Security Readiness Indicator. Whilst these indicators are a positive reflection of the existing journey, cyber security is not "set and forget". The Department and NSW Government will remain focused on building cyber resiliency and on continuous improvement.

The Department seeks to continually improve the Policy and other processes used to assist reporting entities, including through supporting documentation and guidance. The NSW Audit Office's reports this year continue to be a reminder that there is still much work to be done. With the assistance of agencies like the NSW Audit Office, the Department will continue to engage with reporting entities to assist in uplifting their cyber security culture.



Emma Hogan
Secretary

Date: 21/10/21

Response from the Department of Education



DGL21/282

Ms Margaret Crawford
Auditor-General for New South Wales
Audit Office NSW
PO Box 12
SYDNEY NSW 2001

mail@audit.nsw.gov.au

Dear Ms Crawford

Thank you for your letter of 17 June 2021, providing a copy of the *Special Audit – Compliance with the NSW Cyber Security Policy*, and requesting a response from the Department of Education.

The Department is dedicated to the safety, integrity, confidentiality, and availability of our data, and has prioritised the ongoing maturity of our Cyber Security capability with its progress regularly reported to the Executive. We welcome the feedback provided by the Audit Report and I am advised the issues identified are being addressed.

We are, however, concerned that publicly tabling the report would provide potential attackers with a roadmap of how and where to attack NSW Government departments and agencies, and in our case, increase the risk profile to students and staff, which is inconsistent with our strategy.

As you are aware, the Department is currently responding to a significant ongoing cyber incident. Whilst we support the report's findings in principle and are addressing the comments regarding the Department, we would strongly recommend that the full Audit Report not be publicly tabled. This would compromise our current recovery efforts and the inevitable risk of increasing cyber activity exceeds the benefit of placing this information on the public record.

Yours sincerely

A handwritten signature in black ink that reads 'G Harrison'.

Georgina Harrison
SECRETARY
DEPARTMENT OF EDUCATION
15 July 2021



NSW Department of Education

105 Phillip Street Parramatta NSW 2150

GPO Box 33 Sydney NSW 2001

1300 679 332

education.nsw.gov.au

Response from the Department of Planning, Industry and Environment



Planning,
Industry &
Environment

Office of the Secretary

15 July 2021

Ms Margaret Crawford
Auditor-General for New South Wales
GPO Box 12
SYDNEY NSW 2001

Via email: mail@audit.nsw.gov.au

Dear Ms Crawford,

Special Audit: Compliance with the NSW Cyber Security Policy

Thank you for the opportunity to provide a formal response for inclusion in the final report to be tabled in Parliament.

I acknowledge this audit incorporates findings related to nine agencies including the Department of Planning, Industry and Environment (DPIE) and their respective compliance with relevant requirements for the NSW Department of Customer Service Policy 'DCS-2020-02 NSW Cyber Security Policy'.

The Digital Information Office (DIO) of Corporate Services of DPIE has several comments in relation to the report that we request are considered prior to finalisation.

With respect to the reported levels of maturity for DPIE, these were determined through interviews and evidence collection by an independent external Auditor rather than through an internal self-assessment, which was not recognised in the audit report. Notwithstanding DIO acknowledges the identified discrepancies between the reported level of maturity and the level DIO was able to demonstrate with evidence sufficient for the Audit office team for two CSP mandatory controls. It is pertinent to note that these discrepancies were identified in only two out of twenty CSP mandatory controls while all ratings for the Essential 8 strategies were consistent.

DIO was directed by both the independent auditor and Audit office audit teams and supplied all evidence requested. The conclusions of both teams were reached based on this evidence. Although justification for the maturity rating established by the Audit Office for two CSP mandatory controls was provided, the criteria used to determine maturity levels was not shared with DIO. As such, DIO is not in a position to determine the basis on which of the two independently assessed maturity ratings more readily reflect current state. Nonetheless, DIO will adopt the more conservative rating provided by the Audit office for the FY19/20 reporting as final. DIO will continue engaging an external vendor to evaluate annual levels of maturity and will enhance

the compilation and retention of artefacts necessary to determine levels of CSP maturity utilising CSP guidance.

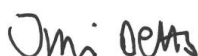
DIO opposes the potential publication of sensitive information about maturity levels including the Essential 8 strategies and requests that these remain confidential and not be publicly released by the NSW Audit Office on security grounds. Advice from the Australian Cyber Security Centre confirms that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities. Publication of CSP and Essential 8 maturity levels and specific mitigations will unnecessarily expose DPIE and equip adversaries with the core information to compromise agency systems. If reporting is required to be published then we request this is done in an aggregated and deidentified manner to reduce, although not eliminate, potential security risks.

Furthermore, a mandatory minimum maturity level of '3' as outlined in the Audit Office report is not a requirement in the Circular, Policy or Guidance. The policy is consciously risk-based requiring agencies to develop practical and realistic security goals and spend their resources in the most effective way depending on key risk areas as opposed to having a minimum standard required to be met by all participants.

DIO management acknowledges that ongoing enhancement of the maturity of CSP controls is required, especially in relation to the ACSC Essential 8 strategies. Since the establishment of the DPIE cluster in July 2019, DIO has embarked on the simplification and modernisation of its ICT environment with security and privacy by default as its priorities. In addition to this, with the initial \$5m DRF cyber security funding granted in March 2021, DIO has commenced a 12-month journey to further uplift DPIE's/DRNSW's cyber security maturity through the delivery of 20 initiatives. One of the initiatives is to develop a Treasury business case for the remaining funds, to cover Phase 2 of the Program, which would take potentially another 2-3 years. In this way, DPIE is prioritising improvements to its cyber security resilience as a matter of urgency.

I would like to acknowledge the important work undertaken by your team and the professionalism they demonstrated throughout this process.

Yours sincerely,



Jim Betts
Secretary

Response from the Department of Regional NSW



Regional
NSW

Your Ref# D2111088

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2001

21 July 2021

Dear Ms Crawford

RE: Compliance with the NSW Cyber Security Policy

Thank you for your letter of 17 June 2021 and the opportunity to respond to your audit report *Compliance with the NSW Cyber Security Policy*. The audit provides valuable insight for the ongoing improvement of cyber security resilience across the Sector.

As you would be aware, Regional NSW was created on 2 April 2020 and while fully accepting its accountability and responsibility for managing cyber security relied (as it still does) on the Department of Planning, Industry and Environment for much of its IT infrastructure and security.

Having said that, Regional NSW has continued to address and strengthen its cyber security controls in line with the *NSW Cyber Security Policy* and believe the current level of maturity to be appropriately higher than at the time of the audit.

Regional NSW note and accept the two specific audit findings attributed to Regional NSW and have taken steps to address these issues as part of the overall maturity process.

Lastly, it is our strong preference for the findings of this report to not be available publicly. We are committed to increasing our cyber security maturity and believe that the findings of your report should be handled internally, so to not flag any potential weaknesses to adverse actors.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Gary Barnes'.

Gary Barnes
Secretary

1 Monaro Street, QUEANBEYAN NSW 2620 | www.regional.nsw.gov.au | 1

Response from the Ministry of Health



Health

Ms Margaret Crawford
Auditor General of NSW
NSW Audit Office
GPO Box 12
SYDNEY NSW 2001

Your ref D2111091
Our ref H20/112992

Dear Ms Crawford

SPECIAL REPORT COMPLIANCE WITH NSW CYBER SECURITY POLICY

I refer to your letter of 17 June 2021 seeking comment from NSW Health on the special audit report *Compliance with the NSW Cyber Security Policy*.

As you are aware the NSW Government's Cyber Security Policy and its application is evolving. NSW Health has worked diligently on the implementation of the requirements of the policy and will continue to work closely with Cyber Security NSW in its ongoing development.

I would like to highlight the leadership of eHealth NSW in the application of policy requirements and in the work undertaken to seek independent assurance on the integrity of NSW Health's cyber security frameworks. The information presented in your report will be considered as part of the ongoing efforts in this area.

I note that this report has been provided for review as a final version, which is a departure from the established process of distributing a draft report first and seeking agency feedback on any areas of disagreement. In context of this, I wish to highlight two key areas of concern.

First, I highlight the sensitivity of the report content and request your discretion in publishing detailed findings which may put the integrity of agency cyber security frameworks at risk. I am aware that this concern has been raised during the conduct of the audit by representatives of NSW Health and other participating agencies.

Second, I also wish to highlight NSW Health's position regarding its performance in the report. Based on the extensive evidence that was provided in the course of this audit, the discrepancies regarding the Audit Office's assessment of compliance with the Cyber Security Policy have not been sufficiently identified or explained. As such, it remains unclear as to what evidence was found to be insufficient and how the assessments made in the report were determined.

Despite this, NSW Health is committed to prioritising work to enhance our cyber security maturity and will continue to work closely with Cyber Security NSW and our colleagues in other NSW Government agencies to achieve this.

NSW Ministry of Health
ABN 92 697 899 630
1 Reserve Road, St Leonards NSW 2065
Locked Mail Bag 2030, St Leonards NSW 1590
Tel (02) 9391 9000 Fax (02) 9391 9101
Website: www.health.nsw.gov.au

Please find attached to this letter further comments in response to the audit recommendations.

Yours sincerely

A handwritten signature in black ink, appearing to read 'EKoff', written in a cursive style.

Elizabeth Koff
Secretary, NSW Health

Encl.

20/7/21

No.	Recommendation	Response	Comment
<i>Cyber Security NSW should:</i>			
1.	<p>Monitor and report compliance with the CSP by:</p> <ul style="list-style-type: none"> obtaining assurance over the accuracy of self-assessments requiring agencies to resolve inaccurate or anomalous self-assessments where these are apparent. 	-	<p>Currently assurance is provided to Cyber Security NSW through the Attestation Statements which were strengthened by NSW Health during the reporting period to reflect the accuracy of the status on self-assessment.</p> <p>NSW Health will work closely with Cyber Security NSW in relation to any perceived deficiencies in complying with the Cyber Security Policy.</p>
2.	<p>Require agencies to report:</p> <ul style="list-style-type: none"> the level of maturity for each mandatory requirement they have determined appropriate for their agency the agency head's acceptance of the residual risk where the target levels are low 	-	NSW Health will address this issue in consultation with Cyber Security NSW.
3.	<p>Identify and challenge discrepancies between agencies' target maturity levels and the risks of the information they hold and services they provide.</p>	-	<p>NSW Health has recognised the value in improving its maturity level consistent with the Cyber Security Policy and will work closely with Cyber Security NSW.</p> <p>NSW Health has prioritised activities aimed at increasing its maturity levels consistent with the Cyber Security Policy and has set appropriate targets for its Cyber Security Uplift Program, which will be progressed in collaboration with Cyber Security NSW.</p>
<i>Participating agencies should:</i>			
4.	<p>Resolve the discrepancies between their reported level of maturity and the level they are able to demonstrate with evidence:</p> <ul style="list-style-type: none"> compiling and retaining in accessible form the artefacts that demonstrate the basis of their self-assessments referring to the CSP guidance when determining their current level of maturity. 	Disagree	<p>NSW Health has reported their level of maturity based on evidence held and has appropriately attested to this as required under the Cyber Security Policy.</p> <p>Based on the extensive evidence that was provided by NSW Health in the course of this audit, the discrepancies regarding the assessment of compliance with the policy have not been sufficiently addressed nor identified to come to this conclusion.</p>

No.	Recommendation	Response	Comment
5.	<p>Cyber Security NSW and NSW Government agencies need to prioritise improvements to their cyber security resilience as a matter of urgency</p>	Agree	<p>This will be addressed by activities being undertaken as part of the new Essential 8 uplift program.</p>

Response from the Treasury



Treasury

Ms Margaret Crawford
NSW Auditor-General
GPO Box 12
SYDNEY NSW 2001

Dear Ms Crawford

Special Audit – Compliance with the NSW Cyber Security Policy

Thank you for the opportunity to provide a response to your Report, *Special Audit – Compliance with NSW Cyber Security Policy*.

I acknowledge your key findings and recommendations. NSW Treasury has addressed the agency specific issues identified in the Report and has an approved uplift plan in place to raise cyber security maturity.

I share the concerns raised by Cyber Security NSW and other NSW Government agencies regarding the external publication of your Report in its current form. I am advised that the detail it contains would provide an advantage to adversaries seeking to target the NSW Government and increase the risk of a successful cyber-attack.

I trust the Audit Office is exploring options with Cyber Security NSW to reduce this risk while enabling transparent and accountable reporting to Parliament, such as creating a public summary version of the Report and making the full version available to Members of Parliament on a confidential basis.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Michael Pratt', written over a light blue grid background.

Michael Pratt AM
Secretary

14 July 2021

Response from Transport for NSW (TfNSW)



Transport
for NSW

Your ref: D2110328
Our Ref: OTS20/07456

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2000

Response to Special Audit – Compliance with the NSW Cyber Security Policy – Final Report

Dear Ms Crawford

Thank you for the opportunity to respond to the Special Audit Report (the Report) on compliance with the NSW Cyber Security Policy (the Policy). Transport for NSW (TfNSW) welcomes the findings of the Report and the confirmation that the evidence we provided substantially supports our assessed cyber security maturity ratings.

Since the release of the Policy in February 2019, TfNSW has been working closely with Cyber Security NSW to implement the Policy and strengthen our cyber defence capabilities. We will continue to work with them in accordance with the Policy to further improve our organisational and operational cyber security maturity to protect our customers, our staff and our critical infrastructure.

In the current cyber security environment of forever changing threats and high-profile cyberattacks on all types of organisations in Australia and overseas, TfNSW recognises the need to continuously improve our cyber defence capabilities to protect our staff, the NSW Government, and the people of NSW.

While further uplift is still required, TfNSW's cyber security controls already effectively prevent a significant number of intrusion attempts and our teams constantly monitor our cyber security environment and respond rapidly to cyber security threats.

We are pleased to advise that we are aware of the shortcoming of the self-assessment and reporting processes under the Policy and have already made improvements. Evidence is now retained to support our self-assessed maturity ratings. Independent sample reviews of critical self-assessments are conducted to ensure maturity ratings are assessed in accordance with the Policy's guidance and are based on adequate evidence.

We have been, and will continue improving, our cyber security resilience. From July 2020 through to June 2023, Transport will have invested an additional \$60 million to support the ongoing uplift of our Cyber Defence Portfolio. In addition, \$20 million will be allocated to the Cyber Defence Program from the Digital Restart Fund to further uplift Cyber security.

Transport for NSW

231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | F 02 8202 2209 | W transport.nsw.gov.au | ABN 18 804 239 602

Cyber security training is mandated for all staff. In addition to formal training, we frequently communicate with staff across the Transport cluster about cyber security risks. Furthermore, we have also improved our threat intelligence and response capabilities to proactively detect and prevent potential threats. We are also instigating further uplift in our organisational structure to embed cyber security culture across our organisation by having divisional IT security teams working closely with our business to improve their cyber security maturity.

This journey of continuous improvement and maturity uplift across one of Australia's largest and most complex government entities demonstrates our focus and commitment to cyber security resilience. Our current and future investments will continuously reduce our cyber security risks.

If you have any further questions, Fiona Trussell, Deputy Secretary Corporate Services, would be pleased to take your call. I hope this response has been of assistance.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Rob Sharp', written in a cursive style.

Rob Sharp
Secretary

10 July 2021