NSW Electoral Commission

The Hon. Tara Moriarty, MLC
Chair
Portfolio Committee No. 1 – Premier and Finance
NSW Parliament
Macquarie Street
SYDNEY NSW 2000

BudgetEstimates@parliament.nsw.gov.au

30 March 2021

Dear Ms Moriarty

ANSWER TO QUESTION TAKEN ON NOTICE ON 4 MARCH 2021

On 4 March 2021 I appeared as a witness at a hearing of the Portforlio Committee No. 1 and took the following question on notice:

QUESTION –

The Hon. JOHN GRAHAM: Mr Schmidt, I am going to interrupt you at that point but only to ask this question, although I am going to ask you to take it on notice. On that cybersecurity point, can you tell us on notice, just give us some sense of the advice you might have got in your discussions with the Australian Electoral Commission or with some of those Federal security agencies you have talked about or with your international counterparts about some of the risks that you are worried about? Obviously, do so appropriately—so be sensitive to what you do and do not want in the public domain—but if you could give us some of that information, I think that would be very helpful, perhaps on notice though.

Mr SCHMIDT: Could I suggest a slightly alternative approach with your indulgence?

The Hon. JOHN GRAHAM: Absolutely.

Mr SCHMIDT: Arising out of the Public Accountability Committee report, there is a recommendation that the issue of funding for State general elections, including integrity and threats, goes to the JSCEM for a further hearing. There are a number of cyber issues et cetera that I would like to explore more fully in that forum and perhaps in camera.

The Hon. JOHN GRAHAM: In fact, I have given notice of exactly that motion in the House. I am asking for this information so the House might properly consider exactly your proposal. If you were able to provide some information on notice, that would be helpful.

231 Elizabeth Street SYDNEY NSW 2000 | GPO Box 832 Sydney NSW 2001
T 1300 135 736 | **elections.nsw.gov.au**

Mr SCHMIDT: As you can see, I am a bit sensitive about exposing some of these in a broader forum, but put the question on notice and we will see what we can come back to assist in the deliberation.

The CHAIR: Are you going to provide the answer on notice? It is just for the records of the meeting.

Mr SCHMIDT: I will take the question on notice and see what I can provide with the caveats that we have talked about to the extent that I feel it a reasonable thing to do.

I now provide my answer below to this question:

ANSWER:

Inter-jurisdictional collaboration on cyber security and elections

Given the potential national security implications arising from electoral system compromises, the NSW Electoral Commission (the Commission) does not share specific information about its cyber security arrangements publicly or with foreign electoral bodies, with the limited exception of the New Zealand Electoral Commission. The New Zealand Electoral Commissioner is a member of the Electoral Council of Australia and New Zealand (ECANZ). The Australian member bodies of ECANZ, of which I am the current Chair and which includes the Australian Electoral Commission, have actively promoted to First Ministers the need for a more co-ordinated approach with federal security agencies around supporting the integrity of all Australian elections, particularly in relation to cyber security. Those efforts have led to the establishment, with the endorsement of the former Council of Australian Governments (COAG), of the Interjurisdictional Working Group on Electoral Integrity and Security (IWGEIS). They have also led to engagement with Commonwealth's Electoral Integrity Task Force in support of recent State elections, including the NSW state general election in 2019.

One of the important items of work supported by COAG was the commissioning of a point-in-time assessment of the cyber security maturity of Australian electoral management bodies. That October 2018 review concluded that the Commission had a low level of maturity against the standards for cyber security – called the Essential 8 - established by the Australian Cyber Security Centre (ACSC). The review also noted that:

> *"The main concern is not the actual damage that cyber attacks can cause to individual electoral system components, although it exposes the individual jurisdiction to significant reputational damage. The bigger concern is that any reports of attempted or successful breaches gives adversaries the ability to sow doubt in the security and integrity of electoral processes. Therefore, an attack on one part of the system must be seen as an attack on the system as a whole....To maintain public trust and faith in democratic processes, it is imperative that actions are undertaken to ensure that all elements of electoral processes are provided sufficient protection."*

Although the specific recommendations of that review are not public, the review concluded that electoral systems are critical national infrastructure and should be protected as such. In this context, on 18 February 2019 the Prime Minister issued a public statement that:

> *"Australia's democratic process is our greatest asset: our most critical piece of national infrastructure."*

Another vital piece of work currently being overseen by the IWGEIS is the development of a proposal for a national electoral platform. The purpose of such a platform would be to provide a more secure technology platform and system capabilities for managing components of electoral infrastructure in Australia.

Collaboration with Cyber Security NSW

With the upcoming September 2021 NSW local government elections in mind, the Commission is actively engaged with Cyber Security NSW (CSNSW). Although the overall risk of cyber breaches to Commission systems are considered to be lower for a local government election, because the national security implications of such elections are also lower, the scale of these elections and the planned introduction of iVote, means the threat level remains significant.

The types of cyber threats that CSNSW and the Commission are presently focused on mitigating in this context, within their respective existing resources, are:

- *More frequent breaches of core systems of organisations, such as network, security or messaging services.* Recent major examples of worldwide significance are the SolarWinds and Microsoft Exchange compromises. These types of breaches are having a serious impact across sectors and regions. They illustrate how there can be waves of continuous exploits following an initial breach. For the Commission to be able to manage these consequential impacts requires mitigation at both broader and deeper levels than is presently the case, with a considerably higher investment of resources needed. Due to the lack of specific funding, however, the Commission must continue to take a reactive approach to these types of threats, rather than preventing them from impacting on our systems in the first place. This means that it may take significant time and resources to respond to incidents if they occur. Mitigation of such an incident is likely to have a major adverse impact on the Commission's capacity to function around election periods.

- *The inherent risks of legacy systems of organisations being exposed and exploited more regularly.* This is a particular risk to the Commission, which has a dependency on a number of bespoke and aging core election systems that were not designed with a security focus in mind and have limited support available. The vulnerability of these systems arises from both their technological age and key person dependencies. There are multiple such systems deployed as part of the Commission's election delivery activities, raising a significant risk from a security assurance perspective.

- *The recent proliferation of nation state actors undertaking sophisticated cyber security activities, including against state and federal Australian institutions, with*

unlimited resources capable of systemic-level impact. The increase in this type and level of activity over recent years make monitoring, detection and response capabilities even more essential before and during each election. Lack of such capabilities, as a result of its long-term funding position, makes the Commission and NSW elections vulnerable to this threat. The significant risk of the 'unknown unknowns' also has the potential to undermine the legitimacy of all election results, which is fundamental to the stability of the NSW democratic system. During the upcoming local government elections, the Commission will rely heavily on CNSW as the source of threat intelligence and advice, as well as the conduit under current arrangements, with the ACSC. The Commission will also need to rely on CSNSW for its assistance with guidance and support in its incident response.

- *A fast-moving technology landscape means security solutions can change rapidly.* With its current limited capability, the Commission is always 'playing catch-up' with technology advances. Investing in more strategic planning to manage the technology risks is therefore essential. The development by organisations, including the Commission, of strategic security roadmaps would lead to fewer *ad hoc* responses to technology risks. Without this type of strategic planning being properly funded, however, there is an ongoing risk of increased technology complexity and sub-optimal security investments. It also seriously limits the capacity of the Commission to innovate in the delivery of elections and its regulatory functions.

Funding to address cyber security threats

As part of this year's State Budget process, the Commission has again sought specific funding to defend the integrity of the State's electoral systems against cyber security threats. The Commission was not successful in its previous three funding proposals to address this issue, other than for a small amount of "seed funding" to develop a further business case (which was subsequently not approved) and the costs of hosting iVote at the 2019 State election in an IRAP-certified secure facility. Lack of adequate investment in the cyber security of NSW electoral systems and personnel over time has meant that the Commission does not comply, and cannot comply in the immediate future, with the NSW public sector's mandatory cyber security policies. The Commission also does not meet the ACSC's Essential 8 standards for cyber security.

Risks to the Commission's cyber security are managed to the limited extent possible from within the resources allocated through the State Budget for the core services of the Commission, being the delivery of elections, management (with the Australian Electoral Commission) of the NSW electoral roll, and regulation of political participants and lobbying. To determine what technical and strategic responses may be available to it from within these resources, the Commission undertakes its own assessment of national and international threats, as well as collaborating where feasible with CSNSW and Commonwealth agencies responsible for national security, such as the ACSC.

To improve the Commission's capacity to respond to these threats, both now and in the future, its 2021/22 Budget proposals seek funding for the following specific additional cyber security measures:

- Improvements to identity and access management to ensure all people who access our systems are correctly identified and have the appropriate level of access. Upgrades to existing systems are required to support improved access management capability.
- Improvements to incident identification and management capabilities through use of an external cyber security operations centre and improved internal capability.
- Resolutions to ongoing cyber security issues with existing legacy systems.
- Ongoing training and process improvement to increase cyber security awareness.
- Updating the Commission's Information Security Management System (ISMS), based on ISO27001:2013, to work towards compliance with the NSW Government's Cyber Security Policy.
- Continue working towards compliance with the ACSC's Essential 8, with a target maturity of at least 2 by the State general election in March 2023.
- Ensure that "security by design" principles are included in the Commission's design and development processes for all new systems.

The Commission is also seeking Budget funding to mitigate the risks associated with its dependency on the more than 50 internally-developed business systems that are critical to delivery of every election. These systems require urgent updates for cyber security, reliability and supportability reasons. Only with additional funding now can the Commission ensure these systems are capable of delivering the 2023 State general election, as well as undertake longer-term critical system planning to protect them into the future. System issues occurred during the delivery of the State election in 2019, these issues directly impacted voters voting at early voting centres. Without immediate investment, the risk of system errors or failures will be increased for the next State election to an unacceptably high level.

If provided, additional Budget funding for systems modernisation will enable:

- Resolution of known issues within existing applications to extend their life so that they will be more reliable during delivery of SGE2023.
- Improved data architecture and data management within existing systems to reduce complexity and make the systems easier to maintain.
- An interface management solution to manage data transfer between the 50+ business systems, increasing reliability and reducing the risk of data errors.
- A long term plan (10+ years) for system asset management and replacement to support future enhancements and the provision of enhanced online services.

Yours sincerely,

John Schmidt

Electoral Commissioner

231 Elizabeth Street SYDNEY NSW 2000 | GPO Box 832 Sydney NSW 2001
T 1300 135 736 | elections.nsw.gov.au