Submission No 4

ADEQUACY OF THE FUNDING ALLOCATION OF THE NSW ELECTORAL COMMISSION FOR THE 2023 STATE GENERAL ELECTION

Organisation: Department of Customer Service

Date Received: 7 February 2022

Department of Customer Service Submission to the Inquiry: "Adequacy of the funding allocation of the NSW Electoral Commission for the 2023 State General Election"

The Department of Customer Service (DCS) welcomes the opportunity to provide a submission to the Joint Standing Committee on Electoral Matters Inquiry into the adequacy of the funding allocation for the NSW Electoral Commission for the 2023 State General Election.

This submission outlines the role of DCS and related engagement between Digital.NSW and the NSW Electoral Commission in the Digital Restart Fund (DRF) application process, including the provision of funding from the DRF for cyber security uplift. This submission does not extend to broader government decision-making on funding for the NSW Electoral Commission, including NSW elections. Such decisions are a matter for NSW Treasury and the Expenditure Review Committee (ERC).

Digital.NSW, within DCS, was established to foster a culture of innovation and customer-centric service design across the NSW public sector. Digital.NSW leads NSW Government reforms across the public sector in the areas of innovation and better regulation to help achieve better customer, policy, and financial outcomes.

Two branches within Digital.NSW have engaged with the NSW Electoral Commission to progress a submission seeking funding from the DRF specifically for cyber security uplift: ICT/Digital Investment and Assurance (IDIA); and Cyber Security NSW.

ICT and Digital Investment and Assurance (IDIA)

ICT and Digital Investment and Assurance (IDIA) administers the DRF. The DRF funds ICT and digital projects using iterative, multi-disciplinary approaches to plan, design and develop digital products and services in NSW. It encourages projects that use agile and flexible procurement methodologies and fosters customer-driven business transformation and collaboration across NSW Government.

The DRF includes a reservation of funding for projects focused on the implementation or improvement of cyber security capabilities. The DRF supports digital transformational projects and is not intended to cover business-as-usual technology run costs, physical infrastructure, operating technology, or multi-year funding proposals.

IDIA are responsible for providing independent assurance of business cases seeking funding as required by the ICT and Digital Assurance Framework. IDIA take a risk-based approach when delivering independent oversight of NSW Government ICT projects. This approach enables critical issues to be identified, regular reviews of projects at various checkpoints (gates) and scope to intervene to ensure projects are delivered on-time, on-budget, and in accordance with NSW Government objectives.

The ICT Assurance team within IDIA provided in-depth analysis of the iVote solution prior to the last election, as well as advice on scalability, stability and general ICT resilience. ICT Assurance continue to support the NSW Electoral Commission through ICT Assurance Framework and Gateway Reviews, including iVote and Gate 2 Review of the cyber security uplift business case. ICT Assurance have referred an expert reviewer to the NSW Electoral Commission, at arm's length, to assist with preparation of a Lean Business Case (seeking less than $5 million in funding) for cyber security uplift. Further support will be provided to assess

and respond to the Gate 2 Review recommendations. In addition, ICT Assurance is working with the NSW Electoral Commission to provide ongoing assurance for their wider ICT program.

Cyber Security NSW

Cyber Security NSW provides an integrated approach to preventing and responding to cyber security threats across NSW; safeguarding our information, assets, services and citizens. Cyber Security NSW aims to build stronger cyber resilience across the whole-of-government to support our economic growth, prosperity and efficiency.

Cyber Security NSW works with IDIA to review business cases seeking funding for cyber security uplift to ensure projects do not duplicate existing whole-of-government initiatives. Cyber Security NSW also advises agencies where initiatives may be of limited value or low priority and identifies any other concerns requiring consideration. This review is in collaboration with the above-mentioned independent assurance of business cases as required by the ICT and Digital Assurance Framework.

Election Integrity and Foreign Interference

Elections are high-interest events that can attract malicious cyber activity. In 2020, the US National Intelligence Council found an increase in network compromises targeting state governments prior to the election day[1]. Risks of electoral interference are relevant for both federal and state government bodies in Australia.

An increasing number of countries are pursuing a cyber espionage program as this offers high returns for relatively low cost and plausible deniability[2]. The continued evolution of technology increases the sophistication and complexity of attacks, while also becoming increasingly accessible.

Malicious threat actor activity may pose a risk to NSW Government if the confidentiality, integrity or availability of election systems is compromised. This could result in a loss of trust in the validity of election results. Any interference or disruption to the ability of the NSW Government to hold elections could have widespread reputational and social consequences.

To combat the evolving cyber security threat landscape and to strengthen the security posture of the NSW Government, clusters and agencies have embarked on the development and implementation of cyber security uplift programs.

NSW Government has led the country in addressing this problem by funding cyber security uplift in the form of a $240 million investment over three years for clusters. Subsequently, in July 2021, an additional $75 million was announced for small agencies. The NSW Electoral Commission is eligible to receive funding from this allocation once DRF requirements are met and the submission is endorsed by the DRF Steering Committee and a committee of Cabinet.

Cyber security maturity uplift takes time. All comparative jurisdictions in the developed world are facing identical difficulties implementing strengthened cyber security capabilities in

[1] https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf
[2] Counter Espionage and Foreign Interference | Australian Security Intelligence Organisation (asio.gov.au)

an environment where cyber threats are rapidly expanding and evolving, and budgets are constrained.

NSW Electoral Commission Digital Restart Fund Bid

The NSW Electoral Commission, like all government agencies and industry, must focus on cyber resilience and continuous improvement. The development of a business case by the NSW Electoral Commission, dedicated to cyber security uplift, is a means by which this focus can continue.

Following the announcement of the additional $75 million DRF allocation for cyber security uplift for small agencies, IDIA advised the NSW Electoral Commission of timelines to progress its business case for Gate 2 Review and subsequent submission to the DRF Steering Committee for consideration.

IDIA and Cyber Security NSW reviewed and provided advice on three iterations of the NSW Electoral Commission "scale" business case (seeking greater than $5 million in funding).

In July 2021, Cyber Security NSW successfully sought in-principle endorsement from the DRF Steering Committee for reservation of funding from the cyber security uplift pipeline for the NSW Electoral Commission, subject to ICT and Digital Assurance Framework requirements being met.

The independent ICT and Digital Assurance process, comprising a panel of representatives commissioned by IDIA and NSW Government, conducted a Gate 2 Assurance Review of the "scale" business case and made critical recommendations for the NSW Electoral Commission to address prior to progression of the business case for approval. Critical recommendations must be remediated to ensure risks are addressed, including those associated with the anticipated successful delivery of the uplift program.

In response to this process, the NSW Electoral Commission developed a Lean Business Case which will enable commencement of work on the first phase of cyber security uplift initiatives, while considering the most appropriate response to the broader Gate 2 Review recommendations.

At the time of submission, the Lean Business Case for the first phase was expected to be submitted for approval in February 2022.

Additional Engagement with the NSW Electoral Commission

Throughout 2021, Cyber Security NSW provided complimentary services to support the NSW Electoral Commission's overall cyber security posture. Some of these services included:

- policy guidance on data sovereignty
- assessments of external facing vulnerabilities
- password hygiene checks, identifying compromised passwords and security concerns with user accounts
- several targeted intelligence assessments focussing on potential cyber security risks that could impact the perceived or actual integrity of elections, and

- on-election-day monitoring supporting the Upper Hunter by-election in May and NSW council elections in December 2021.

Cyber Security NSW have also agreed to provide the NSW Electoral Commission with:

- NSW Cyber Security Policy assistance via the Governance Risk, and Compliance team, and
- general cyber security awareness and training.

Cyber Security NSW supports efforts to enhance the cyber security maturity and capabilities of the NSW Electoral Commission. These improvements will strengthen our coordinated response to threats posed by foreign interference and electoral integrity.

Contact

If the inquiry would like to discuss issues relating to the administration of the Digital Restart Fund (DRF), Mr Mark Howard, Executive Director ICT and Digital Investment and Assurance (IDIA), can be contacted via e-mail at [redacted] or [redacted].

Cyber security-related matters can be directed to the NSW Government Chief Cyber Security Officer, Mr Tony Chapman, via e-mail at [redacted] or [redacted].