Submission No 2

INQUIRY INTO CYBERSECURITY

Organisation: Local Government NSW

Date Received: 18 September 2020

LOCAL GOVERNMENT NSW

Draft submission to the Inquiry into Cybersecurity

Local Government NSW (LGNSW) welcomes the opportunity to provide a submission to the Portfolio Committee 1 – Premier and Finance Inquiry into Cybersecurity.

LGNSW is the peak body for local government in NSW, representing all NSW general purpose councils and related entities. LGNSW facilitates the development of an effective community based system of local government in the State.

This is a draft submission awaiting review by the LGNSW Board. Any revisions made by the Board will be forwarded to the Inquiry Secretariat.

The LGNSW submission focusses on Terms of Reference **1 (j)** *The support provided by the NSW Government to local councils and other organisations in relation to cybersecurity.*

All levels of government and industry are being increasingly targeted by cyber attacks that could put pressure on critical infrastructure and public services.

The NSW local government sector is responsible for the provision of a wide range of essential infrastructure and services and manages infrastructure and land assets worth more than $153 billion. The sector is increasingly relying on technology for information management and acknowledges that information technology controls and governance frameworks are essential to ensure that IT systems are protected from inappropriate access and misuse.

However, to date there has been a complete lack of NSW Government support to local governments in managing cybersecurity threats.

In the *Report on Local Government 2019*, the NSW Auditor-General called for the Office of Local Government to develop a cyber security policy by 30 June 2021 to ensure a consistent response to cyber security risks across councils after finding that 80 per cent don't have a cyber security framework.

The Audit Office of NSW is also planning to undertake an audit within the next three years to consider how well selected councils ensure they have effective cybersecurity measures in place[1]. As noted by the Audit Office, the increasing global interconnectivity between computer networks has dramatically increased the risk of cybersecurity incidents. Such incidents can harm local government service delivery and may include the theft of information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent.

LGNSW supports the development of a cybersecurity policy and governance framework for local government and also advocates for the provision of standardised cybersecurity training.

As well as the provision of a cybersecurity framework, councils also need resourcing support. Councils can experience challenges in attracting skilled workers, particularly in rural and regional areas. In research conducted by LGNSW in 2018, 86% of councils in NSW were experiencing a skill shortage and 69% were experiencing skills gaps. The key reasons for skills shortages were the inability to compete with the private sector on remuneration, lack of suitably qualified/experienced candidates, regional/remote location, high demand across the labour market, and pressure from key major external projects/developments.

---

[1] https://www.audit.nsw.gov.au/annual-work-program-2020-21

LGNSW recommends the State Government address skill shortages and impediments to employment by working with TAFE NSW and registered training organisations to develop and deliver accredited training programs in specialist skill areas such as cybersecurity.

LGNSW welcomes the announcement of increased funding for Cyber Security NSW and the extension of its scope to cover councils and small agencies. LGNSW also supports the current priorities of Cyber Security NSW to expand intelligence capabilities, implement security policy, conduct the annual cyber security exercise program, provide a skills pathway and raise awareness.

While the $60 million investment in Cyber Security NSW is a good start, LGNSW also calls on the NSW Government to provide direct financial support to councils to help improve their cybersecurity capabilities.

The compounding impacts of unprecedented drought, bushfires, floods and the COVID-19 pandemic, coupled with rate pegging and cost shifting, means that council finances are stretched to the limit. Councils need additional financial support from the NSW Government in order to effectively improve their cybersecurity capabilities.

LGNSW appreciates the opportunity to provide a submission to the Portfolio Committee 1 – Premier and Finance Inquiry into Cybersecurity.

For further information, please contact Kelly Kwan, Executive Manager, Advocacy at