

Mr Jason Li MP
Chair
Committee on the NSWICAC
Parliament of NSW

By Email: icaccommittee@parliament.nsw.gov.au

6 March 2025

Our Ref: A24/0029

Dear Mr Li,

**Answers to Questions Taken on Notice - Parliamentary Joint Committee Review of the
NSW ICAC Annual Report 2023-24**

I refer to ICAC's appearance before the Committee for its review of the 2023-24 annual report on 10 February 2025. The Commission's response to questions taken on notice are set out below.

QON 1: Transcript page 6 - Cyber Security industry standard testing

Response:

The Commission addressed this issue in answer to supplementary questions taken on notice in respect of committee's review of the 2021-22 and 2022-23 annual reports. The Chief Commissioner wrote to Mr Li on 9 January 2024 advising:

- 1. Can you comment on the Commission's cyber-readiness and ability to respond to any cyber-security threats and risks, and measures you plan to introduce to improve the Commission's cyber-readiness.***

The Commission complies with the NSW Cyber Security Policy which outlines the mandatory requirements and responsibilities that all NSW Government agencies must adhere to in order to ensure cyber security risks are appropriately managed.

Each year the Commission conducts a cyber security maturity assessment. The Commission's "crown jewels" have been identified, and a cyber security attestation is provided and appears in the annual report (see page 76 of the 2022-23 annual report).

OFFICIAL: Sensitive - NSW Government

Findings from the cyber security assessment are used to develop goals to improve maturity levels within the Commission.

Cyber security matters are communicated and discussed via a number of different committees and forums within the Commission including a monthly meeting with the CEO. Cyber security is a regular item on the Audit and Risk Committee meeting agenda and a report is provided at each committee meeting. A corporate risk register exists which addresses cyber risks and their associated mitigation strategies which are regularly reviewed and managed.

The Commission has documented a security incident response plan and playbook containing instructions to detect, respond, contain and recover from an information security event. Annual cyber security incident response exercises are undertaken simulating real world cyber incidents. This allows the Commission to regularly test its cyber security incident response plan and take proactive measures to identify any gaps in the people, process and technology domains. The following is also relevant:

- An Information Security Management System (ISMS) has been implemented to manage information security using a standard framework.*
- Development of a Cyber Security Awareness program that includes ongoing cyber security training for all staff, regular email communications and simulated phishing exercises*
- Annual penetration testing is conducted where remediation actions are identified and managed through to implementation.*
- The Commission has processes in place to act on information and intelligence received regarding security threats.*

The implementation of the mandatory requirements within the NSW Cyber Security Policy includes implementation of the Australian Cyber Security Centre's Essential 8 controls. In terms of vulnerability and patch management, vulnerability scanning is performed and there is a process for identifying and mitigating missing patches across the network. An automated method of asset discovery is regularly performed and reviewed and deployment of software patches for operating systems and applications is conducted on a regular basis. The Commission has successfully implemented application control within the technology environment, with this including the development of associated processes for the review and installation of approved software. The Commission has implemented permission-based access controls and privileged access management processes are in place.

Tools are used to monitor and identify cyber security events with endpoint security controls installed and active on all end point devices. This includes detection/prevention software providing real time reporting & alerting. Security policy controls are in place for the use of the Commissions internal IT systems and the Microsoft 365 environments, and there are measures in place to ensure security baselines remain consistent with Commission policy. Security event logs are retained and accessible for review with monitoring and alerting processes in place. In addition, the Commission has specific audit tools in place that capture

all activity on IT systems, including desktops, laptops and access to IT systems. VPN access to the network is enforced and multi factor authentication (MFA) is used by the Commission. The Commission has a dedicated disaster recovery site, and backup and recovery processes exist and are reviewed regularly.

There are a number of measures planned to improve the Commission's cyber readiness.

These include:

- continue to implement remedial actions to comply with the CSP and EB mandatory requirements.*
- uplift cyber security risk management to ensure it is considered in all areas across the Commission.*
- boost cyber security awareness including the rollout of targeted face-to-face cyber security training.*
- further develop the ISMS to improve processes and strategies to enable the appropriate response to evolving security threats.*
- continuously assess resourcing requirements whilst taking into consideration constantly changing environmental factors.*

QON 2: Transcript page 7 - Data Retention and Management

Response

All records and information collected during an investigation is referred to as 'property'. The Commission's property management policy states that property collected during an investigation "...is retained by the Commission only for so long as its retention is reasonably necessary for the purpose of an investigation, prosecution or disciplinary proceeding to which it is relevant."

When an investigation is closed, a property disposal workflow is initiated in the Commission's case management system to ensure that property is disposed of.

If there are criminal or disciplinary proceedings arising from a Commission investigation, the property is retained until the conclusion of the proceedings.

The Commission has limited storage capacity for electronic data so once a criminal advisory brief of evidence is forwarded to the ODPP, or records have been provided to a government agency for disciplinary proceedings, the retained data is archived.

QON 3: Transcript Page 7 - Artificial Intelligence in investigations

Response

The Commission has initiated a project to procure a new electronic evidence processing and review platform. This will involve an assessment of our current and future needs. The next generation of these platforms have inbuilt AI capability to assist with the review and analysis of data.

QON 4. Transcript Page 10 – Section 11 Reports/Data Management – access of records

Response

The vast majority of privacy breaches/improper access of records relate to the access of patient records (a large-scale system) by employees who do not have authorisation or a business reason to do so. Most of these are identified through audits conducted by Local Health Districts and therefore controls are in place. In terms of other types of inappropriate access, when we receive reports of this nature we seek to examine what controls are in place to restrict access or to audit access and follow up with agencies/councils accordingly.

The Commission does not have separate categories for types of improper access of records (small scale vs large scale systems) however these can easily be distilled into categories for the purpose of tracking trends. Other factors that are considered are the purpose of accessing the information, the extent of the access (one record vs numerous records) and whether the information was shared and for what purpose.

QON 5. Transcript pages 17-18

Local Council/Development Applications – recommendations to Council on best practice/Independent Planning panel

Response

Although they are not identical concepts, the expression “planning proposal” is typically used interchangeably with “rezoning”.

The Commission’s reports on its *Investigation into the conduct of the City of Canada Bay Council mayor and others* (November 2023, Operation Tolosa), *Investigation into the conduct of three former councillors of former Hurstville City Council, now part of Georges River Council, and others* (August 2023, Operation Galley) and *Investigation into the conduct of councillors of the former Canterbury City Council and others* (March 2021, Operation Dasha) all make findings of corrupt conduct concerning the involvement of councillors in planning proposals. Accordingly, there are clear corruption risks associated with planning proposals, especially those that confer financial benefits on developers.

As noted in those investigation reports, planning proposals are prepared by a local council but are “made” by the Minister for Planning or their delegate. Page 13 of the Operation Tolosa report notes “*After a planning proposal is prepared, the council may forward it to the minister responsible for the planning portfolio to seek a key decision known as a “gateway*

determination". The purpose of a gateway determination is to make an early assessment about whether the commitment of further time and resources is justified and to eliminate proposals that lack apparent merit. The Department has delegated authority from the minister in respect of a gateway determination and determines, among other things, whether the planning proposal should proceed (with or without variation), whether it should be resubmitted for any reason (including for further studies or other information) and the minimum period for public exhibition".

Further, as noted on page 14 of the Operation Tolosa report "During 2018, a new ministerial direction meant that all councils were required to consider the advice of the Local Planning Panel before determining whether to forward a planning proposal for gateway determination". Consequently, local planning panels are already involved in the assessment process, albeit not as the final decision-maker.

The Minister also has powers under Part 9 of the *Environmental Planning and Assessment Act 1979* to take enforcement action against local councils, including by removing their planning functions.

Based on this existing involvement of the Minister, their department and local planning panels, the Commission has not recommended that councillors' involvement in planning proposals be removed. In Operation Galley, the Commission made one corruption prevention recommendation that mentioned planning proposals:

That the DPE amends the Model Code of Meeting Practice for Local Councils in NSW to require a council's governing body to provide reasons for approving or rejecting development applications, planning proposals and planning agreements where decisions depart from the recommendations of staff. These reasons should refer to the relevant merits criteria and explain why the decision is more meritorious than the recommended outcome.

The Department (now the Department of Planning, Housing and Infrastructure) accepted the recommendation but implementation is pending as the Model Code of Meeting Practice for Local Councils is currently under review.

In Operation Dasha, the Commission recommended that the Department improve the gateway determination process by considering corruption risks, taking measures to verify that councils have complied with gateway conditions and establishes a program of regular risk-based auditing (see recommendation 17).

Planning panel members are public officials and it is worth noting that the Commission has not made a finding of corrupt conduct about such an official. However, given the benefits to be gained from rezoning land and approving development applications, any approval authority could be a target. One area of risk that arises in the Commission's work involves the "revolving door" phenomenon. Officials with planning powers (which can include council-employed planners and planning panels members) sometimes find themselves in conflict of interest situations when they move back and forth between the public and private sector roles.

The Commission also notes that the Operation Dasha report recommended that all provisions of the *Lobbying of Government Officials Act 2011* be applied to local government. This recommendation is yet to be implemented. Lobbying practices featured in the *Commission's Investigation into the conduct of the local member for Drummoyne* (July 2022, Operation Witney), which also involved a planning proposal. In this report, the Commission made findings of corrupt conduct in respect of an MP's use of his official position to benefit his family's property interests.

The Commission does closely monitor corruption allegations and risks associated with the way councillors and councils exercise planning functions. On pages 128/129 of the Operation Tolosa report the Commission stated that planning related investigations:

. . . account for nearly half of the total published since 2018. In addition to these investigations, the Commission has referred a number of other allegations involving local councillors and property developers to the OLG for its consideration.

Corrupt conduct involving the environmental planning system and its intersection with councillor decision-making is not isolated to NSW. It has been a focus for other anti-corruption commissions in other Australian states, notably the Queensland Crime and Corruption Commission's 2017 report, Operation Belcarra – A blueprint for integrity and addressing corruption risk in local government, and the Victorian Independent Broad-based Anti-corruption Commission's 2023 report, Operation Sandon – Special report involving the City of Casey Council.

The Commission considers that its reports and those in other Australian jurisdictions emphasise the high-risk nature of environmental planning and property development in terms of corruption. In particular, recent investigations suggest that there are too many elected officials with close connections to development applicants, which may represent a systemic problem.

Implementing the corruption prevention recommendations made by the Commission in this and previous investigation reports involving planning matters will go some way in addressing opportunities for corrupt conduct. However, if necessary, the Commission may decide to take further action in this area.

Finally, it should be noted that there are some local councils at which councillors determine development applications (DAs). Local planning panels determine DAs in the Sydney metropolitan area and at Wollongong, Central Coast and Wingecarribee councils.

QON 6. Transcript pages 17-18 – ICAC's Submission to the Councillor Framework Review

Response

The Chief Commissioner met with Minister Hoenig on 2 December 2024. A copy of the Commission's submission to the Office of the Local Government is available upon request.

QON 7. Transcript page 19 – Section 10 Referrals

Response

The data below shows the breakdown between Councillors and/or Council staff in section 10 reports about local government received by the Commission from July 2023 to June 2024.

s.10 reports concerning Local Government (1 July 2023 – 30 June 2024)	Approx %
Total s.10 Local Government reports concerning Councillors	30
Total s.10 Local Government reports concerning Council staff	41
Total s.10 Local Government reports concerning Councillors and Council Staff	19
Total s.10 Local Government reports concerning private persons or where no subject is named	47

Should you require further information please do not hesitate to contact me.

Yours sincerely,



**The Hon John Hatzistergos AM
Chief Commissioner**