Law Council
OF AUSTRALIA

Business Law Section

2 October 2025

National Office of Cyber Security
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

By email: NOCS.PAA@homeaffairs.gov.au

Dear Sir/Madam,

Code of Practice for Cyber Incident Response Providers

1. The Media & Communications Committee of the Law Council of Australia's Business Law Section (the **Committee**) welcomes the opportunity to respond to the Department of Home Affairs—National Office of Cyber Security's proposed voluntary Code (the **draft Code**), which has been co-designed by the National Office of Cyber Security, the Australia Signals Directorate (**ASD**) and industry. In view of the limited time to respond, this submission combines overarching views with some targeted responses.

Overarching views

2. The draft Code has been thoughtfully prepared with a focus on practical guidance. It is intended to be adopted by providers specialising in the technical component of cyber incident response and on the assumption that information-sharing with the ASD, Australian Cyber Security Centre (**ACSC**) and National Cyber Security Centre (**NCSC**) will be consistent with the 'limited' use regime set out in the *Intelligence Services Act 2001* (Cth) and the *Cyber Security Act 2024* (Cth). The concern the Committee has previously raised in relation to the limited use regime remains under this Code. There is no legal immunity provided in exchange for the information-sharing efforts and there is a high probability of breaching obligations of confidentiality and waiving client legal privilege. This brings tension between a range of legal rights, obligations, voluntary codes of practice and the rule of law.

Targeted responses

Definitions

3. The Code is intended to be adopted by cyber security incident response providers. A cyber security incident response provider is defined broadly as 'usually an external organisation that provides direct and timely assistance in the remediation and future prevention of cyber incidents'. This definition refers only to remediation and future prevention, yet a common theme in the Guiding Principles is 'containment' which incident responders also play a role in supporting during an

incident, as demonstrated in Guiding Principle 2(a) and (d) and Guiding Principle 3.

4. Accordingly, we suggest changing the definition to:

   Cyber security incident response providers—'an internal cyber security specialist or external organisation that provides direct and timely assistance in the detection, containment, remediation and future prevention of cyber incidents'

Guiding Principle 1:

5. The basis for the exclusion of pre-incident detection from the scope of the Code is unclear. A voluntary code of practice intended to help 'prevent and respond effectively to cyber incidents' (Introduction) is better served by a more holistic appreciation of cyber security services and incident response. To be truly effective, providers would inform their clients that failure to build operational understanding and install effective monitoring tools will impede their ability to respond and contain incidents when they occur. Lawyers also require a full picture of what has occurred in a breach in order to be able to advise on the legal ramifications from notifications to reporting, disclosures and mitigation.

6. Accordingly, we suggest the following additional words:

   (a) Applying technical and operational expertise to 'detect, contain and/or assess the cyber security impacts of the incident.'

Guiding Principle 2:

7. Both when clients engage incident response providers and providers respond, there should be a process to ensure client legal privilege attaches to the relevant information needed to undertake the legal assessment and any other action to be taken to ensure compliance with the Code (without loss of confidentiality or waiver of client legal privilege). The Committee suggests consideration be given to adding a sub-clause or amending sub-clause (e) as follows:

   (e) Ensuring that investigative actions are conducted in a way that:
   (i) allows a client to obtain legal advice:
   (ii) preserves client legal privilege (by limiting distribution and sharing of client-specific incident reports or any similar reports produced for another purpose, disclosure of which would have the effect of waiving privilege and losing confidentiality);
   (iii) respect other legal boundaries and data handling requirements.

Guiding Principle 3:

8. Sub-clause (b) states: 'Advising on tailored containment strategies that consider the client's operation priorities and risk tolerance'. Some containment strategies present unique risks. In particular, we suggest that those who adopt the Code be required to advise their clients on the effective duration of a containment strategy (e.g., hours, days, weeks), and the risks of any approach that involves delaying containment for the purpose of gathering evidence.

9. Sub-clause (d) refers to ‘preserving key artefacts’ to ‘support future forensic or regulatory investigations, including potential sharing with ASD’s ACSC or other authorised bodies’. The Committee would object to this without protection of privilege and confidentiality—the incident response providers are engaged by the affected party, not the government.

Guiding Principle 4:

10. Sub-clause (d) states that ‘[w]here possible, preserving relevant artefacts and indicators that may assist ASD or other authorised bodies in broader threat analysis or defensive operations, contributing to the protection of the Australian economy’. ‘Where possible’ does not provide sufficient clarity around the risks of losing client legal privilege and confidentiality that broad disclosure brings—the responders are engaged by the affected party, not the government.

Guiding Principle 5:

11. Sub-clause (c) states that the incident response provider should assist their clients by ‘monitoring for signs of reinfection or residual threats during and after the recovery phase, if within scope’. Incident response providers should also advise clients about the impacts of not monitoring during recovery phase.

Guiding Principle 6:

12. The Committee does not support sub-clauses (b), (c) and (d) as drafted. They are too focussed on the primacy of assisting government and would create a tension between the incident response provider’s confidentiality obligations to its paying clients and compliance with the Code. If providers are able to share information about a cyber incident and the response to it on a de-identified basis, then this issue may be partly resolved.

Guiding Principle 7:

13. The Committee does not support sub-clause (b). This is also focussed on the primacy of assisting government and would again create a tension between the incident response provider’s confidentiality obligations to its paying clients and compliance with the Code. If providers are able to share information about a cyber incident and the response to it on a de-identified basis, then this issue may be partly resolved.

Guiding Principle 8:

14. The Committee suggests consideration be given to adding wording that underscores that the incident response provider cannot use information learned in one incident for the benefit of another client unless the information is de-identified or confidentiality is waived.

New Guiding Principle 9:

15. In our members’ experience, the incident response community is known for oversharing confidential details of investigations under the guise of “threat intel”, without consideration of the implications for clients such as loss of confidentiality and loss of client legal privilege. We suggest consideration be given to adding a

"Guiding Principle 9" for "Confidentiality". This would be framed such that incident response providers may share legitimate threat intelligence provided it is de-identified and only provided to those incident response providers who have signed-up to, and demonstrated consistent compliance with, the Code. There should also be a requirement that: 'Under no circumstance should incident response providers disclose the content of discussions held in a crisis management team, cyber incident response team, IT incident management team or any legal or executive team (however described)'.

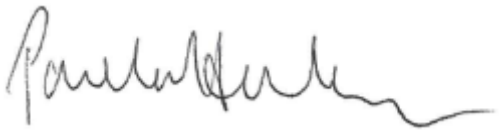
16. Finally, no consequences or enforcement mechanisms are contemplated for non-compliance with the voluntary Code. While a voluntary code by its nature is limited in effectiveness, given the overall objective of the Code, this seems to be in misalignment with the high stakes that a 'limited use' regime poses for clients and providers who participate, without legal protection or legal accountability.

Conclusion and further contact

17. The Committee would be pleased to discuss any aspect of this submission.

18. Please contact the chair of the Committee Marlia Saunders [redacted] or Committee member Lisa Fitzgerald [redacted], if you would like to do so.

Yours faithfully



Professor Pamela Hanrahan
Chair
Business Law Section