



natsiwa

NATIONAL ABORIGINAL AND
TORRES STRAIT ISLANDER WOMEN'S ALLIANCE

Briefing Paper

Cyber Security for Small and Medium Sized Businesses and Organisations

National Aboriginal and Torres Strait Islander Women's Alliance (NATSIWA)
February 2026

Purpose

This briefing paper provides an overview of the Australian Government inquiry into cyber security for small to medium sized businesses and organisations and identifies key issues relevant to small and medium-sized businesses, not-for-profit organisations, and Aboriginal and Torres Strait Islander businesses and organisations.

The inquiry considers cyber maturity, government guidance, cyber-security standards, access to appropriate cyber-security services, employee training, participation in government and large corporate supply chains, and other related matters.

Submissions to the inquiry closed on **28 August 2026**.

Background

Cyber security is increasingly an essential part of doing business and organisational governance in Australia.

Small and medium-sized businesses and organisations can hold significant amounts of personal, financial, commercial and sensitive information while having fewer resources than large businesses and organisations to protect their systems and information.

Small businesses may manage customer information, financial records, payment information, employee records, supplier information and commercially sensitive material. Not-for-profit organisations may also hold sensitive information about members, communities, clients, program participants and people involved in consultations or research.

www.natsiwa.org.au

Cyber-security expectations therefore need to recognise the different resources, risks and capabilities of small and medium-sized businesses and organisations.

Scale of the Issue

Cybercrime continues to create significant financial and operational risks for Australian businesses and organisations.

The Australian Signals Directorate reported more than **84,700 cybercrime reports in 2024–25**, approximately one every six minutes. The average self-reported cost of cybercrime was approximately **\$56,600 for small businesses and \$97,200 for medium businesses**.

For a small business or organisation, a cyber incident can have a significant impact. Financial losses may be accompanied by disruption to operations, loss of information, reputational damage and loss of trust among customers, clients, members, communities and business partners.

Smaller businesses and organisations can also have less capacity to recover from a significant cyber incident.

Cyber Maturity

Cyber maturity varies considerably across small and medium-sized businesses and organisations.

Many smaller businesses do not have dedicated cyber-security personnel. Owners, managers or general IT providers may be responsible for cyber security alongside other responsibilities.

Similar challenges arise in small not-for-profit organisations, where limited funding and staffing can restrict investment in specialist IT and cyber-security capability.

Cyber maturity should therefore not be assessed simply by whether an organisation has a policy or particular technology in place. Consideration should include whether the business or organisation has the capacity to identify risks, maintain secure systems, respond to incidents and continually improve its cyber security.

Government Guidance and Standards

The Australian Government already provides substantial cyber-security guidance through the Australian Signals Directorate's Australian Cyber Security Centre.

The availability of information is important, but information alone does not necessarily give a small business or organisation the capacity to implement appropriate cyber-security measures.

Smaller businesses and organisations may be required to make complex decisions about secure systems, cloud storage, backups, access controls, software, cyber risks and incident response without specialist expertise.

Cyber-security standards should therefore be clear, practical and proportionate to organisational size and risk.

Government should avoid creating requirements that are straightforward for a large organisation with an internal IT and cyber-security team but difficult or costly for a small business or community organisation to implement.

Access to Cyber-Security Services

Small and medium-sized businesses and organisations frequently rely on external IT and cyber-security providers.

However, purchasing appropriate cyber-security services can itself be difficult. A business without specialist technical expertise must determine what services it needs, whether a provider is suitably qualified, whether recommended products are necessary and whether the price being charged is reasonable.

There is an opportunity for government to improve access to trusted providers, independent advice and affordable cyber-security assessments.

This could particularly benefit small businesses and organisations operating in regional, rural and remote locations where access to specialist services may be more limited.

Employee Training

Employee training is an important component of cyber security.

Employees should understand common risks including phishing, scams, password and passphrase security, multi-factor authentication, suspicious communications and safe handling of information.

However, cyber security cannot be treated primarily as an employee responsibility.

Training cannot compensate for insecure systems, outdated technology, inadequate backups, inappropriate access permissions or insufficient technical support.

Good cyber security requires investment in people, systems, technology and organisational governance.

Aboriginal and Torres Strait Islander Businesses and Organisations

Aboriginal and Torres Strait Islander businesses and organisations may experience the same cyber-security challenges as other small businesses while also operating within distinct cultural, community and economic contexts.

Aboriginal and Torres Strait Islander businesses range from sole traders and small enterprises through to larger Indigenous-owned businesses. Aboriginal and Torres Strait Islander community-controlled and not-for-profit organisations may also hold substantial amounts of personal, community and culturally significant information.

Cyber-security policy affecting these businesses and organisations should therefore recognise **Indigenous Data Sovereignty**.

Indigenous Data Sovereignty concerns the rights of Aboriginal and Torres Strait Islander peoples to exercise authority over data relating to our peoples and communities.

Cyber security is consequently not only about protecting information from theft or cybercrime. Consideration must also be given to who controls information, where it is stored, who has access to it, how it is shared and how Aboriginal and Torres Strait Islander peoples maintain authority over information relating to them.

Government should work directly with Aboriginal and Torres Strait Islander businesses and organisations when developing targeted cyber-security programs, resources and support.

Government Procurement and Supply Chains

Cyber-security maturity is increasingly important for businesses and organisations seeking to participate in government and large corporate supply chains.

Appropriate cyber-security requirements protect government, businesses, customers and the broader supply chain. However, these requirements can also create barriers for smaller businesses.

A small business may have the expertise and capability to deliver a contract but lack the financial resources or technical expertise necessary to meet complex cyber-security requirements or obtain particular assessments and certifications.

This is particularly important when governments are simultaneously seeking to increase procurement from Aboriginal and Torres Strait Islander businesses.

Cyber-security requirements should not unintentionally prevent smaller businesses and Aboriginal and Torres Strait Islander businesses from accessing government and corporate procurement opportunities.

Where higher cyber-security standards are required, government should consider practical assistance to help smaller suppliers achieve those standards.

Funding and Capacity

Cyber security requires ongoing investment rather than a one-off response.

Costs can include secure software and systems, IT support, data storage, backups, cyber-security assessments, staff training, insurance, system monitoring and responding to incidents.

For businesses, particularly micro and small businesses, these costs can be significant.

For not-for-profit organisations receiving government funding, cyber security should be recognised as a legitimate organisational and project cost rather than something organisations are expected to absorb from already limited administrative resources.

Key Policy Considerations

Government should:

1. ensure cyber-security standards and requirements are proportionate to the size, risk and resources of small and medium-sized businesses and organisations;
2. improve access to practical and affordable cyber-security support, including trusted providers and independent cyber-security assessments;
3. support cyber-security capability building for small businesses, not-for-profit organisations and Aboriginal and Torres Strait Islander businesses and organisations;
4. recognise cyber security as a legitimate organisational and project cost within Commonwealth grants and funding agreements;
5. ensure cyber-security requirements do not unnecessarily prevent small businesses and organisations from participating in government and large corporate supply chains;
6. provide practical assistance where small suppliers are required to achieve higher cyber-security standards to participate in government procurement;
7. recognise Indigenous Data Sovereignty in cyber-security policy affecting Aboriginal and Torres Strait Islander businesses and organisations; and
8. develop cyber-security programs and resources for Aboriginal and Torres Strait Islander businesses and organisations in partnership with Aboriginal and Torres Strait Islander people.

Conclusion

Cyber security is essential infrastructure for Australia's small and medium-sized businesses and organisations.

Smaller businesses and organisations must take reasonable steps to protect their systems, customers, employees, members and information. However, expectations must be realistic and matched by accessible guidance, affordable technical assistance and proportionate standards.

Increasing cyber-security maturity should enable small businesses and organisations to participate more confidently in the Australian economy and government supply chains rather than becoming an additional barrier to participation.

For Aboriginal and Torres Strait Islander businesses and organisations, cyber-security policy must also recognise Indigenous Data Sovereignty, cultural authority, self-determination and community trust.

Sources

Australian Signals Directorate, *Annual Cyber Threat Report 2024–2025*.

Australian Signals Directorate, Australian Cyber Security Centre, *Small Business Cyber Security Hub*.

Australian Signals Directorate, Australian Cyber Security Centre, *Cyber Security for Charities and Not-for-profits*.

Australian Charities and Not-for-profits Commission, cyber-security guidance and resources for charities.

Australian Institute of Aboriginal and Torres Strait Islander Studies, Indigenous Data Sovereignty resources.

Parliament of Australia, *Inquiry into Cyber Security for Small to Medium Sized Businesses and Organisations*, 2026.

