national electrical and communications association

National Electrical & Communications Association

Submission to the Inquiry into Cyber Security for Small to Medium Sized Businesses and Organisations

House of Representatives Select Committee on Cyber Security

August 2026

About NECA

The National Electrical and Communications Association, NECA, is the peak industry body representing the electrical and communications contracting industry across Australia.

NECA represents approximately 6,500 businesses nationally. Our membership ranges from sole traders and small family businesses through to major national electrical and communications contractors. Small and medium sized businesses form a substantial proportion of the industry and are central to the delivery of Australia's housing, commercial construction, infrastructure, energy, communications and digital economy.

NECA members design, install, commission, maintain and service the electrical and communications infrastructure upon which Australian communities and businesses depend. This includes homes, hospitals, schools, commercial buildings, transport infrastructure, telecommunications networks, data centres, renewable energy systems, batteries, electric vehicle charging infrastructure, building management systems, security systems, communications networks and increasingly sophisticated, connected technologies.

NECA also plays a significant role in workforce development through Registered Training Organisations, Group Training Organisations and industry training activities.

Cyber security is therefore relevant to NECA and its members in two important ways.

- NECA members are businesses themselves. They are exposed to cyber-crime, business email compromise, fraudulent invoices, payment redirection, data loss, business interruption and reputational harm.
- NECA members also design, install and maintain infrastructure that increasingly connects electrical systems, communications networks, information technology and operational technology.

Cyber security is consequently no longer solely an information technology issue for the electrical and communications industry. It is a business resilience, infrastructure, procurement, workforce, skills and supply chain issue.

NECA welcomes the opportunity to contribute to the Committee's inquiry.

Executive Summary

Australia cannot achieve national cyber resilience without improving the cyber capability of its small and medium sized businesses.

The overwhelming majority of Australian businesses are small businesses. They operate with significantly fewer financial, technical and management resources than governments and large corporations, while becoming increasingly dependent upon digital systems, online services and connected technology.

The policy challenge is therefore not simply to increase awareness of cyber security. Small businesses generally understand that cyber security matters. The more significant challenge is providing them with the capability, resources, trusted advice and practical systems required to manage cyber risk.

Government policy should focus on making SMEs more secure, rather than simply imposing additional compliance obligations.

For many NECA members, the most immediate cyber threat is not a sophisticated attack against critical infrastructure. It is cyber enabled fraud. NECA is aware of circumstances where fraudulent invoices and communications have purported to originate from legitimate businesses or NECA members. These incidents can cause financial loss to customers and other businesses while also creating significant reputational damage, administrative cost and disruption for the legitimate business whose identity has been misused.

NECA members have also experienced difficulty obtaining timely police or enforcement action following cyber fraud. Government appropriately encourages businesses to report cyber crime. Businesses must also have confidence that reporting will lead to a clear pathway for assistance, investigation and disruption where appropriate.

NECA supports a nationally consistent and proportionate approach to SME cyber security.

The Australian Signals Directorate Essential Eight provides an important foundation for improving cyber resilience. Government should continue translating these principles into practical measures that SMEs can implement.

Cyber policy must also recognise that electrical and communications contractors increasingly work with connected physical infrastructure and operational technology. The cyber security requirements applicable to conventional business information technology cannot always simply be applied to operational technology without considering the different risks, technologies and operating environments involved.

NECA already partners with State Governments to assist in delivering cyber security education and training to members. NECA would welcome the opportunity to work with the Australian Government to extend this approach nationally.

Government procurement and major corporate supply chains must also apply proportionate cyber requirements.

Cyber security must not become another mechanism through which obligations designed for governments, asset owners and major corporations are transferred indiscriminately through contracting chains to small subcontractors.

Cyber risk should be allocated according to responsibility and control.

NECA supports practical action that strengthens cyber resilience while preserving SME participation, competition, investment and productivity.

Submission

1. The SME cyber security challenge

Small and medium sized businesses operate in an environment of increasing digital dependence.

Digital systems are now fundamental to invoicing, banking, payroll, customer management, communications, procurement, project management and record keeping. For many electrical and communications contractors, digital systems also interact directly with project delivery and connected infrastructure. However, SMEs generally do not possess the internal capability of large organisations.

A small electrical contractor may employ electricians, apprentices, supervisors, estimators and administrative employees, but may not employ a dedicated cyber security professional or internal information technology team. Many SMEs rely upon external technology providers for core systems and support.

Government expectations need to be sophisticated enough to address genuine cyber risk, while remaining understandable and achievable for businesses without specialist internal capability. NECA considers that cyber security policy should therefore be based upon proportionality, practicality and measurable improvements in resilience.

2. The challenge is increasingly capability rather than awareness

There is extensive cyber security information available to Australian businesses. Government agencies provide significant guidance about cyber threats, good cyber practice, incident reporting and risk management. The continuing vulnerability of SMEs therefore cannot be addressed simply by producing more information.

Recent evidence cited by the Australian Chamber of Commerce and Industry demonstrates the distinction between awareness and capability. Approximately 70 per cent of small businesses identify cyber security as an important digital skill, while only 24 per cent report a high level of capability.

Businesses understand that cyber security matters. Many simply lack the time, expertise, financial capacity or confidence to determine what actions should be prioritised and how those actions should be implemented. Government policy should therefore progressively shift from awareness raising towards practical implementation.

SMEs need clear guidance about what they should do, how they should do it, the order in which controls should be implemented, what reasonable implementation should cost and where trusted assistance can be obtained. Industry associations can play an important role in delivering this support.

3. Cyber enabled fraud and business impersonation

Cyber enabled fraud represents a significant and immediate risk for small businesses. The electrical and communications contracting industry involves a substantial volume of commercial transactions. Contractors issue invoices and progress claims. They pay suppliers and subcontractors. They receive payments from customers, builders, developers and government agencies. They are trusted businesses that are attractive to cyber criminals.

Large sums can move through contracting chains during relatively short periods. These commercial arrangements create opportunities for business email compromise, fraudulent invoices, payment redirection and business impersonation. NECA members have made us aware of instances where fraudulent invoices and communications have purported to represent legitimate NECA members or businesses in excess of $100,000 per transaction via fraudulent purchase orders.

The effects extend beyond the direct financial loss suffered by the recipient of the fraudulent communication. The business whose identity has been misused may suffer reputational harm as do owners and procurement staff.

Customers may initially believe that the legitimate contractor issued the fraudulent invoice. Questions may arise about the security of the contractor's systems. Employees may be required to spend considerable time responding to customers, financial institutions, technology providers, their superiors and authorities. For a small business that has spent many years building its reputation, this can cause substantial commercial harm. Cyber policy for SMEs must therefore recognise protection of business identity and reputation as an important component of cyber resilience.

4. Payment and invoice security

Government cyber security guidance for SMEs should place greater emphasis on practical payment security. Relatively straightforward controls can materially reduce exposure to payment redirection and invoice fraud. Businesses should independently verify changes to supplier bank account details through previously established contact information. Unexpected payment instructions should be independently confirmed.

Businesses should implement appropriate internal payment approval processes. Multifactor authentication should be used for email, financial and other significant business systems. Employees should understand how to identify suspicious invoices, emails and requests to alter payment information. Government education should use practical examples drawn from industries where large volumes of business to business payments occur. Construction and contracting provide obvious examples.

5. Reporting and enforcement

Effective cyber security policy requires both prevention and response. NECA members affected by cyber enabled fraud have experienced difficulty obtaining effective police or enforcement action. This warrants consideration by the Committee.

Businesses are encouraged to report cyber crime. The reporting process can nevertheless appear fragmented from the perspective of an affected SME. A business may need to contact its financial institution, another financial institution, police, Commonwealth cyber reporting services, technology providers, insurers and digital platforms.

At the same time, the business may be attempting to protect customers, secure its systems and respond to continuing misuse of its identity. Knowing where to report cyber crime is important. Knowing what happens after the report is made is equally important. Government should examine whether current arrangements provide SMEs with a sufficiently clear pathway following cyber fraud.

Businesses should understand which agency has responsibility, whether further action will occur, whether additional evidence is required and what practical steps can be taken where fraudulent activity continues.

Particular attention should be given to continuing business impersonation. Where fraudulent invoices or communications continue to use the identity of a legitimate Australian business, there should be an effective escalation pathway to support disruption and enforcement activity. Improved coordination between Commonwealth cyber authorities, State and Territory police, financial institutions and other relevant organisations should be pursued.

6. The Essential Eight and practical SME implementation

NECA supports the Australian Signals Directorate Essential Eight as an important foundation for improving cyber security.

The Essential Eight includes application patching, operating system patching, multifactor authentication, restricting administrative privileges, application control, restricting Microsoft Office macros, user application hardening and regular backups.

The challenge for SMEs is implementation. Government should ensure that implementation guidance remains practical and proportionate. A small business should be able to determine which controls it should implement, what level of maturity is appropriate to its risk profile and what evidence may reasonably demonstrate that the controls are operating. It should not simply become another certification or procurement requirement imposed without consideration of business size, risk and capability.

7. Construction provides an important case study

The construction industry provides a valuable example of the digital capability challenges facing SMEs. Research commissioned by the Office of the NSW Building Commissioner found that 95 per cent of businesses examined were micro, small or medium enterprises. The research also found significant reliance upon informal digital training and outsourced information technology services.

This environment is highly relevant to electrical and communications contractors. A contractor may have limited internal information technology capability while simultaneously installing sophisticated electrical, communications and connected systems. Digital adoption should therefore not be confused with cyber maturity. A business can use sophisticated digital tools or install advanced connected infrastructure without necessarily possessing mature internal cyber security systems. This reinforces the importance of sector specific training and trusted industry delivery channels.

8. Connected infrastructure and operational technology

Australia's cyber security policy must recognise the increasing convergence between physical infrastructure and digital systems. Electrical and communications contractors increasingly work with building management systems, communications networks, energy management systems, security systems, access control systems, smart metering, solar installations, battery systems, electric vehicle charging infrastructure and other connected electrical equipment. Data centres provide a particularly clear example.

Their operation depends upon sophisticated electrical infrastructure, communications networks, control systems, monitoring systems, backup systems and digital technologies. Cyber security policy must therefore consider both conventional information technology and operational technology.

The Essential Eight provides an important information technology security foundation. Operational technology environments can involve different risks, operating requirements and consequences.

Government should work with industries responsible for designing, installing and maintaining connected physical infrastructure to develop practical sector specific guidance. Electrical and communications contractors should be part of that process.

9. Responsibility across technology supply chains

Cyber responsibility must be allocated according to responsibility and control. Small electrical and communications contractors should be responsible for matters reasonably within their control. This includes competent installation, appropriate configuration, responsible handling of credentials and compliance with applicable security requirements. Responsibility for vulnerabilities inherent in equipment design, software, firmware, cloud platforms and manufacturer systems should not automatically be transferred to the installer. Manufacturers and technology providers should retain appropriate responsibility for product security, security updates, vulnerability management and ongoing product support.

Asset owners and network operators similarly have responsibility for the systems they own, control and operate. This reflects a broader principle consistently advanced by NECA in relation to contracting. Risk should sit with the party best able to identify, manage and control that risk. Cyber security should not become an exception to sound commercial risk allocation.

10. Trusted industry partnerships

Australia already has considerable cyber security expertise and guidance. The challenge is ensuring that this expertise reaches SMEs in a form that is trusted, practical and relevant. Industry associations provide an established mechanism for doing so.

Small businesses frequently rely upon their industry association for advice about regulatory changes, technical requirements, workplace safety, training and emerging commercial risks. NECA already partners with some State Governments to assist in providing cyber security training and education to members.

These arrangements demonstrate the practical value of partnerships between government and trusted industry organisations. NECA would welcome the opportunity to work with the Australian Government and relevant Commonwealth agencies to deliver similar initiatives nationally. A Commonwealth partnership with NECA could support industry specific training, workshops, webinars, cyber fraud education, incident response guidance and practical cyber capability tools. This approach would build upon existing government expertise rather than duplicate it. It would also provide government with a direct pathway into thousands of electrical and communications businesses and be replicated further with other specialist trades associations.

11. Workforce capability

Cyber security awareness increasingly needs to extend beyond business owners and specialist technology personnel. Electrical and communications workers increasingly operate around connected devices, communications systems and digitally enabled infrastructure. Appropriate cyber awareness should progressively form part of relevant vocational education, continuing professional development and industry training.

This does not require electricians or communications workers to become cyber security specialists. It requires workers to understand cyber risks relevant to their activities. This may include managing credentials, connecting equipment to networks, configuring remote access, handling customer network information, recognising unusual access requests and understanding when specialist cyber expertise is required.

Training must remain practical and current. Cyber threats and digital technologies can evolve more rapidly than traditional training development processes. Government should therefore support industry led approaches that allow training products and resources to respond quickly to emerging risks while maintaining appropriate national standards.

12. Access to standards

Technical standards can assist businesses to improve governance and cyber security capability yet the cost of accessing standards can itself become a barrier for small businesses.

The Commonwealth has recognised this broader problem through measures supporting access to mandatory Australian Standards. NECA strongly supports the principle that businesses should have reasonable access to standards that government expects them to understand and apply. Government should investigate extending sponsored access to important cyber security standards that provide recognised pathways for improving business cyber resilience, even where those standards are not expressly mandated by legislation.

13. Cost of cyber security investment

Improving cyber security requires investment even where government information and guidance are provided without charge. Implementation may require expenditure on software, backups, security services, professional advice, training and system improvements. These costs are more significant for SMEs because they cannot necessarily spread fixed compliance and technology costs across a large organisation.

Government should consider targeted measures that encourage SMEs to invest in cyber security. This should include consideration of whether the instant asset write off or another appropriate tax mechanism should recognise eligible cyber security software and other defined cyber resilience expenditure.

14. Access to trusted cyber security services

Many SMEs lack the expertise required to assess cyber security providers. A business owner may know that additional protection is required but have difficulty determining what services are necessary, whether a provider is appropriately qualified and whether the proposed cost represents value.

Government should investigate practical mechanisms to improve access to trusted providers. This could include recognised provider arrangements, practical procurement guidance and standard scopes of service appropriate for SMEs. Government support should assist businesses to make informed decisions without creating another complex regulatory regime.

15. Government procurement and supply chains

NECA supports appropriate cyber security requirements for businesses participating in government procurement and major corporate supply chains. These requirements must be proportionate to the actual risk associated with the services being delivered. A contractor with privileged access to sensitive systems or critical operational infrastructure may appropriately be subject to substantial cyber requirements.

A contractor undertaking conventional installation work without access to sensitive information or systems should not automatically face the same obligations. NECA is concerned that cyber security could become another area where enterprise level obligations are transferred indiscriminately through contracting chains. A requirement imposed upon a government agency or major corporation should not automatically flow through to every subcontractor simply because the business forms part of the supply chain. Cyber requirements should reflect the contractor's access, function and capacity to control the relevant risk.

Businesses should know the cyber obligations applicable to a contract before tendering and pricing the work. Cyber requirements should not subsequently be expanded without appropriate consideration of cost, capability, responsibility and risk.

16. Cumulative compliance costs and SME participation

Cyber security requirements do not operate in isolation. SMEs participating in major supply chains can already face substantial procurement and compliance obligations relating to workplace matters, insurance, environmental requirements, sustainability, ethical sourcing, modern slavery, certification and reporting. Their cumulative effect can nevertheless create a substantial administrative burden for smaller businesses without dedicated compliance teams.

Cyber security requirements should therefore be designed with the cumulative compliance burden in mind. Government should seek to avoid duplicate assessments, inconsistent questionnaires and multiple certification processes covering substantially the same risks. Nationally recognised and mutually accepted mechanisms for demonstrating appropriate cyber maturity should be pursued. A contractor should not be required to complete substantially identical cyber security assessments for multiple government agencies and major customers.

17. Cyber maturity must not become a barrier to competition

Poorly designed cyber requirements could unintentionally exclude capable Australian SMEs from government and major corporate procurement. This would reduce competition, diminish local industry participation and increase project costs without necessarily producing better cyber security outcomes.

Advanced certification may be justified where a supplier handles sensitive information or accesses critical systems. It should not become a universal precondition for participation regardless of the work being performed.

Procurement frameworks should support SMEs in improving cyber maturity while preserving genuine opportunities to compete.

18. Cyber insurance

NECA has previously provided detailed evidence concerning small business insurance to the Parliamentary Joint Committee on Corporations and Financial Services inquiry into Small Business Insurance. That inquiry includes cyber threats within its consideration of small business insurance.

NECA does not seek to repeat its detailed insurance evidence in this submission. Cyber insurance can form part of a broader risk management framework. It is not a substitute for appropriate security controls. The theoretical availability of insurance should also not justify transferring cyber risks to SMEs where those businesses cannot reasonably identify, manage or control the underlying risk. Risk should be allocated to the party best able to control it.

19. National consistency

Australia should avoid creating overlapping and inconsistent SME cyber security frameworks. Different requirements imposed by Commonwealth agencies, State and Territory governments, infrastructure owners, government procurement bodies and major corporations would increase cost and complexity.

A nationally recognised baseline should be capable of proportionate application across industries and jurisdictions. Additional requirements should be imposed where genuinely justified by the sensitivity, access or criticality of particular work. National consistency would provide businesses with greater certainty and allow industry associations, training providers and technology businesses to develop scalable solutions.

Recommendations

NECA recommends that the Australian Government adopt the following measures.

1. Establish a clear and nationally consistent SME cyber security baseline based upon practical and proportionate controls, with the Essential Eight providing an important foundation.
2. Recognise that the principal SME challenge is increasingly a cyber capability gap rather than simply an awareness gap, and direct greater resources towards practical implementation support.
3. Develop sector specific cyber security guidance for industries working with operational technology and connected physical infrastructure, including the electrical and communications industry.
4. Establish a stronger national approach to cyber enabled fraud affecting SMEs, with particular emphasis on business email compromise, fraudulent invoices, payment redirection and business impersonation.
5. Review cyber crime reporting and enforcement arrangements to provide SMEs with a clearer pathway to assistance, investigation and escalation, particularly where fraudulent activity or business impersonation is continuing.

6. Partner with trusted industry associations to deliver practical cyber security education directly to SMEs. NECA would welcome the opportunity to partner with the Australian Government, building upon its existing experience working with State Governments to deliver cyber security education to members.
7. Support industry led training development so that cyber security education can respond quickly to changing technologies and emerging threats, while maintaining appropriate national standards.
8. Progressively incorporate relevant cyber security awareness into electrical and communications vocational education, continuing professional development and industry training.
9. Extend Commonwealth sponsored access arrangements to designated business critical cyber security standards where those standards provide recognised pathways for SMEs to improve cyber resilience.
10. Consider targeted tax incentives, including appropriate treatment under the instant asset write off, for eligible cyber security software and other defined SME cyber resilience expenditure.
11. Ensure cyber security requirements in Commonwealth procurement are proportionate to the actual risk associated with the contractor's work and are clearly disclosed before tender.
12. Prevent enterprise level cyber security obligations from being indiscriminately transferred through contracting chains to SMEs that cannot reasonably control the relevant risk.
13. Require procurement frameworks to consider the cumulative compliance burden imposed upon SMEs and minimise duplicate cyber assessments, questionnaires and certification requirements.
14. Develop nationally recognised and mutually accepted mechanisms through which SMEs can demonstrate appropriate cyber maturity across multiple government and corporate procurement environments.
15. Ensure manufacturers, technology providers, asset owners, network operators and contractors remain responsible for cyber risks according to their respective capacity to identify, manage and control those risks.
16. Improve SME access to trusted cyber security expertise and practical guidance for selecting appropriate providers.
17. Pursue national consistency between Commonwealth, State and Territory SME cyber security requirements wherever practicable.

NECA would welcome the opportunity to appear before the Committee and provide further evidence on the experience of electrical and communications contractors and the role the industry can play in strengthening Australia's national cyber resilience.

To arrange a meeting or discuss this submission further, please contact:
Kent Johns
Head of Government Relations and Regulatory Affairs
NECA National

E kent.johns@neca.asn.au **W** www.neca.asn.au