IoTAA submission - **Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy**

September, 2025

To Whom It May Concern,

IoT Alliance Australia submission - **Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy**

Internet of Things Alliance Australia (IoTAA) thanks the Department of Home Affairs for the opportunity to submit feedback to the **Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy**.

The IoTAA is the peak body representing the Australian IoT industry. We encompass the IoT eco-system from IoT service providers, Carriage Service Providers, Industrial IoT (IIoT ~ industry 4.0) device manufacturers and users across industry sectors including transport, smart places and infrastructure, food/agribusiness, health and energy.

Internet of Things technologies and resulting "real-time" data practices have, or are in the process of, entering all industry sectors including the fastest growing consumer environments. The immense opportunity for productivity improvement, new business models, sustainability and employment through application of IoT is counterbalanced by the need to build trust with users and to protect lifestyles and the economy. This includes the protection of individuals, companies and critical infrastructure.

The IoTAA would welcome the opportunity to discuss any aspects of our submission in further detail and how the IoT industry may help to achieve a secure, resilient and trusted Australia.

Yours sincerely,

[redacted]

[redacted]

[redacted]
IoT Alliance Australia

[redacted]

www.iot.org.au

IoTAA submission - **Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy**

Developing our vision for Horizon 2

1. **What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2**?

   There are a number of key trends that will shape the outlook:
   - Technology
     - The increasing adoption of smart devices in both consumer and industrial applications.
     - The advent of quantum technologies which open up the possibility of hyper secure and hyper vulnerable IT and OT scenarios
     - The increasing use of AI technologies and the risks associated
       - Consequential increases in automation without human oversight
       - Risk of poor data and data management fuelling poor decisions
     - Increasing sophistication of cyberattack technologies (e.g. using quantum)
     - Centralising access to data
       - Puts added pressure on strong access controls and identity management systems
   - Policy and Regulation
     - Increasing global security global regulation creating boundaries and zones of control e.g.
       - The evolution of the European Cyber security act
       - US expansion of smart product definition for security labelling
     - The risk of misalignment in global cyber strategies reducing critical threat sharing and collective responses to threats
     - The risks associated of global tech companies control and access to data being compromised to Australia's detriment and with poor transparency and influence on risk management, mitigations and redress

Collaborating across all levels of Australian Government

2. **Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?**

   The Victorian government is considering accrediting the security of smart devices in the water sector for use principally for critical infrastructure to lessen the testing and risk burden for critical infrastructure organisations.

   This has a flow on effect in informing and assisting non-critical infrastructure entities, which nevertheless provide critical infrastructure – e.g. smaller utilities

Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

3. **Does the high-level Model resonate and do you have any suggestions for its refinement?**

Two suggestions:

- New technology developed could be split into new technologies/products etc and new technologies for cyber threats. The latter shifting the threat landscape
- There perhaps should be a feedback loop between targets prepared, cyber attack attempted and the outcomes (blocked or successful). There are often many attack vectors for a product/service and these will change as new threats and threat technologies evolve, as will the outcomes against known protection systems.

4. **Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?**

   There should/could be some form of continuous audit of products and services together with continuous monitoring for evidence of attacks and anomalies.

Shield-level focus for Horizon 2 Shield 1: Strong businesses and citizens

5. **What could government to do better target and consolidate its cyber awareness message?**

The federal government is one of a number of channels to business regarding cybersecurity. Reinforcing messaging through other channels including state governments, service providers, industry associations, user groups etc would help. It is also a way to better target the message to specific groups.

Extend messaging and narrative that is meaningful for different audiences about risks. Australia is behind in its corporate and government cyber security posture. There needs to be a greater sense of urgency that it is about more than loss of data. It's about making sure networks are not rendered inoperable or being maliciously used to damage people and property .

6. **What programs or pilots have been successful in this context?**

The cyberwarden pilot seems a good step in this direction.

7. **What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?**

Extending cyber awareness and education across trades, especially in areas for high growth and technology advancement. E.g. in areas of distributed energy resources (DER)

Possibly raising cyber training as a must have credential in key cross-over trade areas e.g. electricians, installers, maintenance and engineering.

8. **How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?**

Make it way simpler. Perhaps more easily understood recommended layered security levels depending on business risk; and associated security packages/tools and qualified implementers for SMB/NFP cyber-resilience.

9. **How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?**

Industry associations are good vehicles for understanding their constituents needs and for spreading the messages, but are not well resourced to produce the collateral and incentives to improve uptake. Government can help here with collateral and tools and co-designed incentives, or to provide funding for associations to tailor information for their sector/market.

10. **What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?**

There are a host of security standards already available and in development. Relating these to SMB business risk and need, providing clear recommendations and even mandating minimum standards can be a powerful way to assist.

11. **What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?**

NFPs are often poorly resourced and funded. Unless they already have relevant subject-matter expertise, NFPs will need external advice and support to improve their cyber resilience.

12. **Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?**
No response

13. **How well do you consider you understand the threat of ransomware, particularly for individuals and small entities?**
No response.

14. **How is this threat evolving or changing? How could the government further support businesses and individuals to protect themselves from ransomware attacks?**
No response

15. **Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community**

faced? How can support services for victims of identity crime be designed to be more effective in the context of increasing demand?
No response

16. **Which regulations do you consider most important in reducing overall cyber risk in Australia?**

    The evolving SOCI act amendments has made some good impact on awareness and action for entities identified as critical infrastructure organisations.

    Mandatory minimum security standards for smart devices will help raise the base level of security for the vast number of new smart devices. This will take some time to ripple through for great effect as old smart devices are replaced.

17. **Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?**

    No.

Shield 2: Safe technology

18. **What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?**

    Don't know.

    The Standards Australia Roadmap for CER cybersecurity provides some standards context.

    https://www.standards.org.au/documents/roadmap-for-cer-cybersecurity-report

    The Australian Energy Sector Cyber Security Framework (AESCSF) provides an assessment framework and guidance on cybersecurity preparedness of energy market participants such as generators, retailers, networks and the market operator. Currently it lacks sufficient consideration to fleets of CER. While some work has been done to adapt the AESCSF requirements to CER operators, such as in SA Power Networks' Cyber Security Requirements1 for CER operators connecting their flexible export server, consistent design and implementations of guidelines for CER Operators will be essential.
    As the AESCSF is a voluntary assessment, policies and guidance will need to be put in place to ensure operators of large fleets of CER have minimum levels of cybersecurity compliance. There are various state and federal based mechanisms to achieve this.
    https://arena.gov.au/assets/2025/08/CAPA-Intelligence-%E2%80%93-Cyber-Risk-Study-The-Growing-Cybersecurity-Imperative-for-CER.pdf

19. **How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?**

The security labelling scheme for smart devices/products which is due for launch in March 2027, will go a long way in introducing a simpler way of communicating with consumers regarding security for their smart devices.

Helping drive uptake of smart products by preferring labelled products in government procurement could significantly has the profile of labelled products and consumers trust in their selection.

For industry, encourage and support understanding and application of key industry security standards such as IEC 62443, NIST CSF, NERC CIP, ISO 27001.

20. **What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors**?

No response.

21. **How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?**

A couple of potential mechanisms:

- Establish clear guidelines for access rights, identity and distributed data sharing frameworks that limit and compartmentalise data breach impact while easing data access.
- Apply meaningful accountability to data rights holders to protect their data and to limit rights to share data

22. **Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?**

Zero Trust is a foundational principle for securing public sector systems and is generally accepted as the way forward, reflecting global best practice in mitigating identity-based threats.

Implementation is uneven within the public sector and industry seems to be lagging in adoption of the necessary requirements to deliver Zero Trust.

Government can work better with industry to set the example for government agencies and to set workable models for industry adoption for Zero Trust.

23. **What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?**

Guardrails that advise on safe and responsible use are good, but examples of good practice and benchmarks for secure and safe use of critical and emerging technologies will better help uptake.

Shield 3: World-class threat sharing and blocking

24. **What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?**

By highlighting good practices, service providers and technologies.

Demonstrating the above through government purchases(a third of the market!) would further reinforce user understanding and trust on what good is.

25. **Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?**

Government has an important role with industry in helping to set benchmarks for good practice and a proactive security posture. Especially in helping harmonise what that may look like across the states.

26. **How could government further support industry to block threats at scale?**

No response.

27. **How could the use of safe browsing and deceptive warning pages be amplified? What more is needed to support a thriving threat sharing ecosystem in Australia?**

No response

28. **Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?**

Most sectors would seem to be low maturity in terms of sharing cyber and physical threats and mitigation strategies. This includes sectors that are important for critical infrastructure.
This partly due to security risk not perceived as high risk as other important business risks and the absence of a competent well-funded entity that can be the vehicle for curating and sharing across an industry sector.

29. **How can we better align and operationalise intelligence sharing for cyber security and scams prevention?**

No response.

30. **Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?**

    No response.

31. **How could government better incentivise businesses to adopt vulnerability disclosure policies?**

Highlight the good players.

32. **Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?**

No response.

Shield 4: Protected critical infrastructure

33. **How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?**

Partially effective in raising focus on security risks and action on risk management. Our observation is that risk management is unevenly understood and applied across critical infrastructure organisations.

Our observation is that security measures are also not well understood or implemented for IoT systems. This has a double-sided effect:

- It dampens enthusiasm for IoT an Industry 4.0 implementation slowing innovation and productivity outcomes
- In the absence for good security knowledge and capability have been introducing a 'security gap' in utilising data , automation and AI

As a result the SOCI act has the effect of slowing investment and innovation.

Risk management plans seem to be quite varied in quality. Enforcing that there is a plan is ok, but enforcing a good plan (with standards?) is worth considering.

34. **Are there significant cyber security risks that are not adequately addressed under the current framework?**

No response

35. **Is the regulatory burden on industry proportionate to the risk and outcomes being sought?**

    Hard to say and dependent to some degree on issues such as:
    - Relative cost of security for competitors
    - Consumer understanding of security and appetite for risk
    - International security obligations that affect trade

It is important to ensure obligations are simple and effective. We haven't yet cracked what that is.

36. **What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?**

    Improving access to and understanding of benchmarked security risk management good practice and tools to underpin the incentive to invest in appropriate security capability**.**

    Assisting with industry to showcase proportionate security capability versus risk.

37. **How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?**

    Provide better guidance to government procurement for security requirements, including standards, certifications, benchmarks and good practice.

    Making relevant security standards freely available.

38. **How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?**

    No response.

Shield 5: Sovereign capabilities

39. **What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?**

    There are two main areas where government call hep the environment for growth of Australia's cyber workforce on the demand side:
    - Design and product development skills - through government purchase of Australian built cyber solutions, products and services
    - Setting clear benchmarks and standards for cybersecurity and cybersecurity credentials for government and industry to create a pull for skills

    On the supply side to encourage and support of training and education to support he above needs.

40. **What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?**

No direct experience in this, but anecdotally we have seen a number of instances where companies that invest in retraining their staff in digital and cyber skills improve staff retention and lower costs of otherwise expensive external contractors.

One option is a cadetship for mature workers in transition.

41. **What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?**

Industries with highly transferrable skill sets—such as finance, law enforcement, healthcare, IT infrastructure, and project management—are considered excellent sources for talent making the leap into the cyber workforce. There is supporting research and data underscoring the value of non-traditional backgrounds, and highlighting specific pathways and skill types most valued by employers.

Key Industries with Transferrable Skills

- Finance: Professionals possess strong risk assessment, crisis management, and regulatory compliance experience directly aligned with cyber risk management and audit roles.

- Law Enforcement & Military: Expertise in investigation, intelligence gathering, threat analysis, communication, and attention to detail maps closely to roles in threat hunting, incident response, and security operations.

- Healthcare: Skills in handling sensitive data, regulatory frameworks, and patient confidentiality are relevant for privacy, data protection, and compliance roles.

- IT Infrastructure: Experience as network/system administrators and engineers provides foundational technical skills crucial for cyber job functions such as security architecture, monitoring, and engineering.

- Project Management & Business: Strong organizational, communication, and leadership abilities are vital for cyber project management, governance, policy development, and awareness roles.

Research & Data Supporting Career Transitions

- Reports from organizations like CyberCX and Per Capita highlight a critical skills gap, and advocate for upskilling, academy programs, and diverse entry-pathways—including non-traditional backgrounds—to meet demand.

- Australian and international government workforce plans encourage identification of core skills, adjacent job functions, and provision of clear training pathways from outside professions.

- Academic research indicates that technical ability, combined with skills in communication, business acumen, social intelligence, and adaptability, are key

indicators of success in cyber roles; thus, these are sought in new entrants regardless of previous industry.

- Employers are increasingly valuing practical, transferrable competencies and foundational skills over narrowly defined technical expertise alone, making the field increasingly accessible to career-switchers.

Examples of Valuable Transferrable Skills

- Problem-solving and critical thinking
- Attention to detail, crisis management, and adaptability
- Communication and teamwork
- Data analysis and investigative mindset
- Regulatory and risk-based approaches

In summary, fields rooted in risk management, critical analysis, technical oversight, and communication offer robust on-ramps to the cyber workforce, with data-backed pathways and dedicated training initiatives supporting these transitions at both industry and policy levels.

These are the resources to support the above:

https://www.institutedata.com/us/blog/switching-to-cybersecurity-in-30s/
https://www.upskilled.edu.au/skillstalk/how-to-make-cyber-security-your-new-career-path
https://cybercx.com.au/news/cyber-skills-shortage-approaches-crisis/
https://www.peoplebank.com.au/pathways-into-cybersecurity-is-there-a-right-way-in

42. How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

CRCs seem to be the best model, so far, for genuine industry, academia, think tanks and government to work together. Ideally co-led by industry and research rather than a research lead. The model may need to be tweaked to make it easier for industry to co-invest.

Support Australian research and commercial development of post-quantum cryptographic tools, secure key exchange platforms, and detection systems to reduce reliance on foreign technologies.

43. **How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?**

44. **How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?**

    By prioritising according to:

    - Risk
    - Impact
    - Capability

45. **What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?**

    Of concern is the concentration of hyperscaler platforms and lack of control due to opaque external governance.

    Mitigations could include tying local use to changed governance arrangements that provide better visibility and access locally.

Shield 6: Strong region and global leadership

46. **Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?**

    No response

47. **Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?**

    No response.

48. **Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?**

    No response

49. **In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?**

    No response

50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

Ideally overarching principles that support:

- International trade
- Improvements in visibility and mitigation of global and regional security threat landscapes
- Transparency in the origins of threats
- Cooperation in handling regional and global security breaches
- Cooperation in sharing learnings from regional and global security breaches