The 2023–2030 Australian Cyber Security Strategy (the Strategy) and associated 2023-2030 Australian Cyber Security Action Plan (the Action Plan)

Consultation Paper/Reforms

Contribution by:

Dinesh Velusamy
(Phd (Fintech) Candidate – Federation University Australia, MSc – Cybersecurity – Staffordshire University UK (reading), Masters in IT – Manipal university India)
25 years Tech industry experience

Email:
[redacted]

Dr. Muhammad Imran
Senior Lecturer – Information technology
Federation University
Email:
[redacted]

Part 1 – New cyber security legislation

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices Q1-Q7

1. **Responsibility in the Supply Chain**: Responsibility for complying with a mandatory cybersecurity standard should ideally be shared across the entire supply chain of smart devices. This includes manufacturers, software developers, and distributors. Each entity plays a crucial role in ensuring the security of IoT devices. Manufacturers are responsible for building devices with secure hardware and firmware; software developers must ensure their software is secure and free from vulnerabilities; distributors and retailers should only market and sell devices that comply with these standards.
2. **ETSI EN 303 645 as a Baseline**: The first three principles of the ETSI EN 303 645 standard are an appropriate minimum baseline for consumer-grade IoT devices in Australia. These principles include no universal default passwords, implementing a means to manage reports of vulnerabilities, and providing clear information on the duration of security updates. They establish a fundamental level of security that all consumer-grade IoT devices should meet.
3. **Alternative Standards**: In addition to the ETSI EN 303 645, the government could consider **IoT Security Compliance Framework, OWASP's ISVS** and **ENISA's Baseline Security Recommendations**. However, the choice of standard depends on the specific needs and operational context.

If your focus is on consumer IoT devices and ensuring their security from design to end-of-life in a general context, **ETSI TS 303 645 V2.1** offers the most direct and comprehensive guidance.

For organisations looking for a broad, compliance-oriented approach that covers both technical and governance aspects, the **IoT Security Compliance Framework** from the IoT Security Foundation is recommended.

If your organization prioritises a risk-based approach and requires a scalable standard for securing IoT applications, **OWASP's ISVS** provides an excellent framework.

For IoT deployments in critical infrastructure sectors, where the focus is on resilience and data integrity, **ENISA's Baseline Security Recommendations** offer the most targeted guidance.

1. ETSI TS 303 645 V2.1

Scope: Developed by the European Telecommunications Standards Institute (ETSI), this standard specifically targets the security of consumer IoT devices. It outlines a series of technical specifications and best practices for manufacturers to secure their devices against common threats.

Strengths: It is comprehensive and designed with consumer devices in mind, making it highly applicable to a wide range of products. The standard is well-recognized in Europe and has been influential in shaping IoT security policies.

Limitations: Its primary focus on consumer devices might limit its applicability to the broader IoT ecosystem, especially in sectors dealing with critical infrastructure.

2. IoT Security Compliance Framework from the IoT Security Foundation

Scope: This framework offers a structured approach to assessing and enhancing the security of IoT products. It encompasses a self-certification scheme that enables manufacturers to demonstrate their compliance with best practices in IoT security.

Strengths: The framework is flexible and can be applied across various sectors. It encourages transparency and accountability among IoT device manufacturers.

Limitations: While it provides a comprehensive approach to compliance, the reliance on self-certification might not be sufficient for critical applications without external validation.

3. OWASP Internet of Things Security Verification Standard (ISVS)

Scope: The ISVS by the Open Web Application Security Project (OWASP) offers a tiered security standard for IoT applications, detailing security requirements across different levels of assurance.

Strengths: Its tiered approach allows organizations to apply security measures based on the risk profile and criticality of their IoT applications. It is versatile and can be used in conjunction with other security practices and standards.

Limitations: It might require significant security expertise to implement and interpret, potentially making it less accessible to smaller organizations without dedicated security teams.

4. ENISA Baseline Security Recommendations for IoT

Scope: Developed by the European Union Agency for Cybersecurity (ENISA), this set of recommendations provides a broad framework for securing IoT devices within the context of Critical Information Infrastructures.

Strengths: It covers a wide range of considerations specific to critical infrastructures, making it particularly relevant for government and large organizations managing essential services.

The recommendations are backed by the European Union, offering a solid foundation for regulatory compliance.

Limitations: The broad scope might not provide the level of detail needed for specific implementations without additional, more focused guidelines.

Given the importance of enhancing IoT device security within critical information infrastructures, the ENISA Baseline Security Recommendations for IoT stands out as the premier standard for governmental adoption and enforcement. This standard's focus on safeguarding critical infrastructures aligns perfectly with the imperative to protect vital services and uphold national security. The endorsement by the European Union adds a layer of regulatory credibility, enabling a robust framework for ensuring compliance across diverse organizations and businesses. However, a more holistic, hybrid strategy that amalgamates elements from other notable standards and frameworks, such as ETSI TS 303 645 V2.1's detailed technical specifications for consumer IoT devices and the comprehensive security verification processes outlined by the IoT Security Compliance Framework and OWASP ISVS, is recommended. This integrated approach promises a thorough coverage of security necessities for IoT devices, striking a balance between stringent regulatory demands and the practicalities of implementation. It is essential for governmental bodies to support this adoption through the provision of clear guidelines, compliance assistance, and possibly incentives for organizations that lead the way. This strategy not only facilitates a smoother transition to robust IoT security practices but also ensures a sustained defence against evolving threats, thereby maintaining the integrity of critical infrastructures.

4. the Government could consider other standards like the NIST's Framework for Improving Critical Infrastructure Cybersecurity, which offers a more comprehensive approach to managing cybersecurity risks. Moreover, ISO/IEC standards such as ISO/IEC 27001 for information security management could also be considered for their robustness and international recognition.

5. **Definition of Smart Devices**: A broad definition, subject to exceptions, should be used to define smart devices subject to the Australian standard. This approach allows for flexibility and adaptability as technology evolves. The definition could be similar to the one in the UK's PSTI Act but tailored to address specific vulnerabilities or concerns unique to the Australian context.

6. **Exclusions from the Standard**: Devices that should potentially be excluded from the mandatory cybersecurity standard could include highly specialised industrial IoT devices that are already governed by sector-specific regulations, or low-risk devices where the impact of a security breach is minimal.

7. **Timeframe for Industry Adjustment**: A reasonable timeframe for the industry to adjust to new cybersecurity requirements would be 12-18 months. This allows sufficient time for manufacturers and developers to integrate the necessary changes into their design and production cycles while ensuring that consumers are not left vulnerable for an extended period.

8. **Regulatory Powers Act for Monitoring and Enforcement**: The Regulatory Powers Act does provide a suitable framework for monitoring compliance and enforcement of a mandatory cybersecurity standard for IoT devices. Its existing provisions for regulatory powers, including

monitoring and investigation, issuing infringement notices, and seeking injunctions, can be effectively applied to enforce IoT device security standards.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses. Q8-Q15

8. **Mandatory Information for Ransomware Incidents**:

I. Date and time of the incident.
II. Type of ransomware used.
III. Method of infection and exploited vulnerabilities.
IV. Description of affected data and systems.
V. Impact assessment on operations and data.
VI. Steps taken to respond to the incident.
VII. Whether law enforcement or cybersecurity firms were contacted.

9. **Additional Information if Payment is Made**:

I. Amount and currency of the ransom paid.
II. Payment method used.
III. Communications with the attackers, including any demands or instructions.
IV. Receipt of decryption keys or data return (if applicable).
V. Any follow-up actions post-payment.

10. **Scope of Ransomware Reporting Obligation**:

The scope should include all businesses holding sensitive or personal data, regardless of size, due to the potential impact on individuals and other entities.
For smaller entities, simplified reporting requirements or assistance in reporting could be provided.

11. **Scope Limitation to Larger Businesses**:

Limiting the obligation to larger businesses may overlook significant data breaches in smaller entities. Instead, a tiered approach based on the nature of data held and potential impact could be more effective.

12. **Time Period for Reporting**:

A reporting period of 72 hours from the detection of the incident or ransom payment is appropriate. This allows sufficient time for initial assessment while ensuring timely sharing of critical threat information.

13. **No-fault and No-liability Principles**:

These principles can significantly increase confidence in reporting, as entities would be less concerned about potential legal repercussions or blame for the incident.

14. **Balancing No-fault Principle and Accountability**:

Public communications can emphasize the proactive role of businesses in cybersecurity while maintaining no-fault reporting. Educational initiatives can also encourage best practices without assigning blame.

15. **Enforcement Mechanism**:
Civil penalties for non-compliance can be effective. Additionally, incentivizing compliance through benefits such as faster incident support or access to government resources can also encourage timely reporting.

16.Types of Anonymized Information to Share:

I. Trends in ransomware types and methods.
II. Geographical hotspots of incidents.
III. Effective response and recovery strategies.
IV. Frequency and amount of ransom payments.
V. Frequency of Reporting: Quarterly reports would balance the need for timely information without overwhelming entities. Shared with industry stakeholders and relevant government bodies.

Additional Notes
▪ **Clarification of Reporting Parameters**: Clearly define the threshold for incidents that must be reported to avoid over-reporting of minor incidents that may not significantly impact the broader threat landscape. ▪ **Integration with Existing Reporting Mechanisms**: Ensure that the new reporting requirements seamlessly integrate with existing cyber incident reporting frameworks to reduce duplication and streamline processes for reporting entities.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. **Prescribed Cyber Security Purposes for Limited Use Obligation**:

I. Identifying and analysing the nature and scope of the cyber incident.
II. Providing targeted advice and support to affected entities for incident response and recovery.
III. Enhancing the national cyber threat intelligence and informing future cybersecurity strategies.
IV. Developing and disseminating best practices and preventive measures to the wider community.
V. Facilitating collaboration with international cybersecurity bodies for global threat intelligence sharing.

18. **Restrictions on Use or Sharing of Information**:

I. Information should be used exclusively for cybersecurity purposes and not for regulatory or punitive actions against the reporting entity.
II. Sharing should be restricted to relevant parties directly involved in cyber incident management and response.
III. Personal and sensitive data should be anonymized or redacted to protect privacy and confidentiality.
IV. Information should not be used in a manner that could expose the reporting entity to additional cyber risks or reputational harm.

19. **Incentives for Collaboration and Information Sharing**:

I. Provide timely and practical support to entities reporting incidents, including access to expert advice and resources.
II. Offer cybersecurity improvement grants or incentives for entities that actively engage and share information.
III. Recognize and publicly acknowledge entities that contribute significantly to national cybersecurity efforts.
IV. Develop and maintain a trusted environment where entities can share information without fear of reprisal or negative consequences.
V. Organize regular forums or workshops to facilitate direct engagement and knowledge sharing between government bodies and industry entities

Additional Notes
▪ **Incorporating a Broader Range of Stakeholders:** Include a diverse range of stakeholders, including small and medium-sized enterprises (SMEs), in consultations to ensure the policy is inclusive and practical for all industry segments. ▪ **Regular Reviews and Updates:** Regularly review the effectiveness of the limited use obligation and update it as necessary to respond to evolving cyber threats and industry feedback.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. **Purpose and Scope of CIRB**:

I. To conduct thorough, impartial reviews of significant cyber incidents to understand their root causes and impacts.
II. To provide actionable insights and recommendations for improving cybersecurity practices and policies across industries and government entities.
III. To enhance national cyber resilience by sharing lessons learned and best practices.

21. **Limitations on CIRB**:

I. Should not duplicate or interfere with ongoing law enforcement, national security, intelligence, or regulatory investigations.
II. Operate with a clear understanding that its role is to provide insights for improvement, not to enforce laws or regulations.

22. **Adopting a 'No-Fault' Approach**:

I. Clearly communicate the purpose of the CIRB as a learning and improvement tool rather than a fault-finding body.
II. Ensure reports and recommendations focus on systemic improvements rather than individual blame.

23. **Criteria for Review by CIRB**:

I. Scale and impact of the incident on national security, economy, or public welfare.
II. Novelty or uniqueness of the attack method or its implications.
III. Potential for widespread learning and improvement across sectors.

24. **CIRB Membership**:

I. Members should include cybersecurity experts, industry representatives, and possibly consumer advocates.
II. Appointments should be based on expertise, experience, and ability to provide a balanced perspective.

25. **Expertise of CIRB Members**:

I. Should possess proven expertise in cybersecurity, IT infrastructure, legal and regulatory aspects, and sector-specific knowledge.
II. Diverse representation from different domains like IT, law, cybersecurity, ethics, and industry-specific knowledge.

26. **Managing Security and Conflicts of Interest**:

I. Implement strict conflict of interest policies.
II. Ensure rigorous personnel security measures for CIRB members.

27. **Chair of CIRB**:

I. Should be an individual with extensive experience and respect in the field of cybersecurity or a related field.
II. The chair should be seen as impartial and capable of guiding objective reviews.

28. **Initiating CIRB Reviews**:

I. Initiation could be based on referrals from cybersecurity agencies, industry bodies, or because of significant incidents.

29. **Powers of CIRB**:

I. Powers to request information and cooperation from relevant entities.
II. Authority to publish reports and recommendations.

30. **'Limited Use Obligation' for CIRB**:

I. Similar to ASD and Cyber Coordinator, to protect entities sharing information from liability or regulatory repercussions.

31. **Enforcement Mechanisms for CIRB**:

I. Non-compliance with information requests could result in administrative penalties, but focus should be on voluntary cooperation.

32. **Impartiality and Credibility of CIRB**:

I. Diverse and balanced representation on the board.
II. Transparent processes and clear communication of findings and recommendations.

33. **Integrity and Protection of Sensitive Information**:

I. Implement strict confidentiality agreements for members.
II. Use secure channels for communication and storing sensitive information.
III. Guidelines for handling and disseminating sensitive information, especially in public reports.

Additional Suggestions
▪ **Clear Criteria for Incident Review**: Define clear and specific criteria for what constitutes a significant cyber incident to ensure that CIRB reviews are focused and effective. ▪ **Legal and Regulatory Alignment**: Ensure that CIRB's activities and recommendations are aligned with legal and regulatory frameworks to support effective and lawful implementation of its findings. .

Part 2 – Amendments to the SOCI Act

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data.

34. **Managing Risks to Corporate Networks and Systems**: Effective risk management involves a combination of technical, procedural, and organizational measures. Implementing a layered security approach, including regular vulnerability assessments, threat monitoring, and incident response plans, is crucial. Additionally, employee awareness and training on cybersecurity best practices play a significant role in protecting critical data.

35. **Proposed Amendments to the SOCI Act**: The amendments aim to enhance the security of data storage systems within critical infrastructure. Balancing regulatory burden involves ensuring that the measures are scalable and applicable across different sectors and sizes of organizations, allowing flexibility in implementation while maintaining a high level of security.

36. **Financial and Non-Financial Impacts**: The financial impact includes the costs associated with upgrading systems, compliance activities, and potential penalties for non-compliance. Non-financial impacts involve changes in business processes, data usage, and organizational culture towards a more security-centric approach. The obligations could influence the ability to use data effectively for business purposes, necessitating a review of data management and utilization strategies to align with security requirements.

Additional Suggestions
▪ **Clarification of 'Business Critical Data'**: Define 'business critical data' clearly to ensure a common understanding across all entities and to facilitate effective implementation of the proposed measures. ▪ **Cybersecurity Insurance and Liability**: Encourage or provide guidance on cybersecurity insurance and liability considerations for entities, as part of risk management strategies. ▪ **Incentives for Compliance**: Provide incentives or recognition for early adopters or those who demonstrate exemplary compliance with the new standards.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers.

37.The proposed directions power would enable a rapid, coordinated response to major cyber-attacks on critical infrastructure by providing legal authority and operational clarity. It allows for decisive action and access to government resources, facilitating swift restoration of affected services.

38.The proposed consequence management power would need to align with state and territory emergency management laws, national privacy and data protection laws, and sector-specific regulations. Careful coordination is essential to ensure compliance and effectiveness across different legal frameworks.

39.The government should implement a framework emphasizing transparency, proportionality, accountability, collaboration, privacy protection, and independent oversight. These principles ensure responsible use of consequence management powers, balancing rapid response with respect for legal and ethical considerations.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions. (Q40-Q41)

40. Improvements to the current information sharing regime under the Security of Critical Infrastructure (SOCI) Act could focus on increasing clarity, reducing administrative burdens, and enhancing real-time collaboration capabilities. Suggestions include:

I. **Streamlining Processes**: Simplify reporting requirements and processes to facilitate quicker sharing of critical information without excessive administrative overhead.
II. **Enhancing Real-time Collaboration**: Develop platforms or systems that allow for secure, real-time information sharing and collaboration between government and critical infrastructure entities.
III. **Clarifying Guidelines**: Provide clear, detailed guidelines on what information needs to be shared, with whom, and under what circumstances, to remove ambiguity and promote compliance.

41. **Impact of a 'Harm-Based' Threshold for Information Disclosure**

Moving towards a 'harm-based' threshold for information disclosure could have mixed impacts on decision-making. On one hand, it could simplify the decision process by making it clear that information should be disclosed when there is a potential for significant harm. This clarity could encourage more proactive sharing of critical information. On the other hand, determining the potential for harm might introduce complexities, requiring detailed risk assessments and possibly leading to delays in information sharing.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers.

42. The introduction of the proposed review and remedy powers under "Measure 8: Enforcing critical infrastructure risk management obligations" is poised to significantly influence organizations' approach to preventative risk management. This measure is expected to instil a proactive, compliance-driven mindset, compelling organizations to not only enhance their continuous monitoring capabilities but also prioritize risk management as a core operational focus. Anticipation of external reviews would necessitate the adoption of industry best practices and standards, beyond merely meeting minimum compliance thresholds. Furthermore, organizations would likely bolster their documentation and reporting mechanisms to effectively demonstrate adherence to risk management protocols. In essence, these powers aim to foster a more diligent, structured approach towards mitigating risks, ensuring that efforts are genuinely directed at safeguarding operations and critical infrastructure assets against potential threats.

Additional Suggestions
▪ **Clear Guidelines and Examples**: Provide clear guidelines and practical examples to help entities understand the new TSRMP obligations and how to comply with them.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

43: Security Standards for RMP Development

The most relevant security standards for developing a Risk Management Plan (RMP) in the telecommunications sector include:

I. ISO/IEC 27001: International standard for information security management systems (ISMS), providing a systematic approach to managing sensitive company information.

II. NIST Cybersecurity Framework: Offers guidelines on how to prevent, detect, and respond to cyber-attacks.
III. ITU-T X.805: Specifically designed for telecommunications organizations, this standard provides a comprehensive security framework covering access control, authentication, and network integrity.

44: Interaction with State, Territory, or Commonwealth Requirements

State, territory, and Commonwealth requirements interact with RMP development by providing additional compliance obligations and guidelines that must be integrated into the organization's risk management processes. This could include specific local data protection laws, emergency management regulations, and sector-specific security mandates. Ensuring that RMPs are aligned with these varying requirements necessitates a comprehensive understanding of the legal and regulatory landscape across jurisdictions.

45: Uniform Approach to Notification Obligation through Material Risks Outlining

Outlining material risks can help adopt a more uniform approach to the notification obligation by:
Identifying Common Threats: Highlighting shared threats across the sector can streamline the notification process, making it easier for organizations to understand when a risk reaches the threshold requiring notification.
Standardizing Risk Assessment: Establishing common criteria for evaluating and reporting risks ensures that all entities assess threats in a consistent manner, facilitating clearer communication with the government.

46: Barriers to Government Engagement and Clarification of Notification Process

Main barriers to engaging with the government through the notification process include complex regulatory requirements and ambiguity in what constitutes a notifiable incident. Clarification can be achieved by:

I. Providing Clear Guidelines: Detailed instructions on the types of incidents that must be reported, including examples and thresholds.
II. Simplifying Reporting Mechanisms: Streamlining the notification process through user-friendly platforms and standardized forms can reduce administrative burdens.

47: Alignment with Procurement and Network Change Management Processes

Procurement and network change management processes often require adjustments to align with existing and proposed notification arrangements due to:

I. Dynamic Nature of Threats: Rapid technological changes and evolving threats necessitate flexible and responsive management practices.
II. Compliance Requirements: Ensuring that procurement practices adhere to security standards and that changes in network configurations are promptly reported. Improvements could include:
III. Integrating Security Considerations: Embedding security assessments into procurement processes and establishing protocols for evaluating the security implications of network changes.
IV. Enhancing Communication Channels: Facilitating smoother interaction between technical teams and regulatory compliance units to ensure timely notification and compliance with SOCI Act requirements.

**AI powered Language optimisation tools we used to tweak the language (PaperPal, Gemini)*