FUJITSU

Consultation Response: Horizon 2 - 2023-2030 Australian Cyber Security Strategy

Fujitsu Cyber
Author/s: Sonesh Seddiqi, Alaina Lawson
Editor: Cairo Malet
August 2025

Cover Sheet

Version Control

Version #	Version name	Date
0.1	Response to Horizon 2 - Draft	13/08/2025
1.0	Response to Horizon 2 v1.0	22/08/2025

Contributors

Author/s	Contributor/s	Editor/s
[redacted]	[redacted]	[redacted]

Approval

Approved by	Approval date	Approved to send to (destination)
[redacted]	26/8/2025	Department of Home Affairs

Context

The Australian Government released the *2023-2030 Australian Cyber Security Strategy* on 21 November 2023 (the Strategy).

The Strategy sets up a framework for government to take action to uplift Australia's cyber maturity and preparedness over three horizons, making Australia a world-leader in cyber security by 2030.

- In Horizon 2 (2026-28): we will scale our maturity across the whole economy. We will make further investments in the broader cyber ecosystem, continuing to scale up our cyber industry and grow a diverse cyber workforce.

As we approach the transition from Horizon 1 to Horizon 2, we are developing the actions and initiatives for government to take, together with industry, for the next three years under Horizon 2.

Consultation for Horizon 2

To commence the consultation process on Horizon 2, the Government has released a Policy Discussion Paper for public consultation. The Discussion Paper will continue our collaboration with businesses and citizens on identifying and developing policy options that will best position Australia to be a cyber resilient nation. Fujitsu is committed to this industry co-design process and seek to engage to support this mission.

Introduction

Fujitsu Australia Limited ("Fujitsu") is pleased to respond to the Australian Government's invitation to provide feedback on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. Fujitsu appreciates the Department of Home Affairs strong commitment to engaging a comprehensive stakeholder engagement process as part of the development of Horizon 2.

Given the scale of the proposals under Horizon 2, Fujitsu is focusing its feedback on the key shields / initiatives to provide targeted feedback and actionable insights. Complementing this, we have the below thematic feedback on Horizon 2.

Building on Horizon 1 success, Horizon 2 should consider:

- **Qualification**: how is success of the uplift validated and mapped this across the aggregated shields.
- **Deduplication / Standardisation:** how to reduce the compliance burden and drive control consistency across the digital economy deduplicating requirements across the federal / state / sectors.
- **Simplification**: How to streamline messaging and engagement points for cyber uplift – aiming to simplify the messaging to ensure consumption and clarity.
- **Transparency**: How can the uplift / control requirements be visually mapped to clearly show the alignment of obligations between international, federal, state and sector.

As noted above, our feedback focused on practical measures that build upon Horizon 1 achievements while addressing gaps that remain unfilled, particularly for smaller organisations and entities operating across multiple jurisdictions.

We believe Horizon 2 presents an opportunity for Australia not only to uplift domestic resilience but also shape international alignment and position itself as a partner of choice in the region and beyond.

We would welcome the opportunity to continue working with Government to refine these initiatives and support their implementation.

Consultation Feedback

Sheild 1. Strong Business & Citizens

"Target resilience uplift to small entities that cannot adequately protect themselves, including through giving small business clear and low or no-cost cyber standards to apply."

We commend the Government's progress under Horizon 1 in raising awareness and strengthening preventive measures for smaller organisations. These initiatives have provided valuable foundation for cyber resilience uplift across the economy. However, current offerings under Horizon 1 remain largely prevention-focused, with limited support on the operational documentation and planning that guides a response when an incident occurs.

Most SMBs and NFPs do not have mature, tested artefacts such as Incident response plans, communication templates, supplier assurance checklist, or even basic security policies. The absence of such plans increases downtime and financial loss when an incident occurs and often leaves these organisations reliant on ad hoc responses.

From our experience the challenge is not in awareness or creating resources, but ensuring they have fit-for-purpose tools they can adopt and embed into daily operations.

Recommendations

Develop a Cyber Resilience Documentation Toolkit for SMBs and NFPs, with:

- Business Continuity (BC) / Disaster Recovery (DR) Templates: simplified BC/DR plan, example contract / reporting trees, recovery objectives, short tabletop exercise guides.
- Core Security Policy Pack: lightweight, editable templates written for SMB/NFP scale.
- Supplier Assurance Starter Kit: due-diligence questionnaire and minimum contract clauses.
- Baseline Compliance Checklist: a self-attestable summary organisation can share with insurers, suppliers to demonstrate baseline resilience.

This toolkit compliments Horizon 1 by turning health check outputs into concrete reusable documents. It ensures that small organisations not only understand what to do but also have the artefacts in hand to act when incidents occur.

"Enhance support for citizens and victims of cybercrime to help them bounce back quicker"

It's encouraging to see the Government recognising the critical role of victim support organisations in cyber recovery. This commitment in Horizon 2 signals a welcome shift towards strengthening recovery pathways alongside prevention and detection efforts.

While non-profit victim organisations (e.g. IDCARE) provide invaluable assistance to individuals and businesses, their capacity is often stretched, particularly during large-scale incidents, creating delays at the point when timely action is most critical. These organisations often operate on constrained budgets, which impacts their ability to expand services, develop new capabilities, and respond to surge events.

We recommend dedicated, sustained funding to expand the capacity and reach of trusted victim support organisations. This funding should be tied to structured collaboration frameworks that allows these entities to rapidly draw on additional technical, legal and advisory expertise when required. Such investment would ensure victims receive both immediate guidance and the practical, specialist support necessary for effective recovery.

Recommendations

Provide sustained, dedicated funding to expand the capacity and reach of trusted non-profit victim support organisations, enabling:

- Single support entry portals.
- Sector specific recovery support for SMBs and NFPs.
- Multilingual and culturally appropriate guidance.
- Strong referral pathways from government cyber reporting platforms.
- Rapid access to specialist technical, legal and advisory expertise during major incidents.
- Ability for support organisations to rapidly share (with consent) event information with relevant entities (government, banking, etc.).

The investment would ensure victims receive both immediate guidance and practical, specialist support necessary for effective and timely recovery. It also ensures victims have a central support challenge which can support further engagement as required.

"Harmonise and simplify cyber regulation to promote best practice and efficiency"

Developing a practical cybersecurity baseline for SMBs and NFPs is a sound strategy for lifting national resilience in a proportionate way. Smaller organisations often sit at the intersection of high exposure and low capacity, making them attractive targets for cybercrime, yet often are the least equipped to implement complex frameworks.

Existing standards such as the Essential Eight offer strong direction, but they are often resource-intensive and better suited to large enterprises. Without tailored guidance, many SMBs and NFPs remain unsure of where to start, how to allocate scarce resources, or how to measure maturity over time.

A dedicated baseline designed with clear, prioritised steps, practical templates, and alignment to existing frameworks, would bridge this gap. By being proportionate and accessible, such a baseline would provide smaller entities with an achievable pathway to uplift security practices while still contributing to broader national resilience goals.

Recommendations

Develop and launch a practical Cybersecurity Baseline for SMBs/NFPs, featuring:

- Drive consistency in controls across federal / state / sectors to reduce the compliance burden.
- Baseline, achievable, controls in plain language, ensure these are aligned / mapped to national / international standards.
- Develop clear step-by-step implementation guides and templates.
- Provide clear maturity tiers (e.g. Starter, Growing, Mature) for progressive adoption.
- A one-page "baseline compliance summary" for clients, insurers, and regulators.

This gives smaller organisations a clear, credible starting point for cyber resilience that aligns with established frameworks but is scaled to their capacity.

This also reduces regulatory burden and simplifies an entity's ability to attest to compliance improving insurance and regulatory integration.

Sheild 4. Protect Critical Infrastructure

Horizon 2 Shield 4 sets out two key priorities aimed at strengthening the resilience of Australia's owed and shared critical infrastructure. These priorities are intended to ensure regulatory settings keep pace with the evolving threat landscape, while also driving a more integrated and strategic approach to risk management and investment.

"Mature the regulatory framework for critical infrastructure security"

"Centralise risk management, investment and policy for Commonwealth cyber uplift to drive more coordinated security outcomes"

The implementation of the Security of Critical Infrastructure (SOCI) Act, and its maturity, clearly demonstrates that the Australian government recognises the heightened security imperative for its' critical infrastructure.

The forward-looking focus in Horizon 2 also acknowledges that responses must be sector-specific and proportionate, demonstrating a clear shift toward more context-driven policy. Equally important is the recognition of global interconnectivity and the need for cooperation with international partners on shared assets such as submarine cables and space systems.

However, while the SOCI Act establishes a strong legislative baseline, regulation alone cannot deliver true resilience in Australia's critical infrastructure. Compliance provides the foundation, but uplift depends on continuous collaboration with critical infrastructure operators and the introduction of practical initiatives that move beyond a compliance towards adaptive resilience against evolving adversaries.

Complementing this the Horizon 2 emphasis on centralising Commonwealth cyber security risk management and investment is critical given the scale and interdependence across the Commonwealth's digital estate. The expressed focus on protecting the most critical and significant systems sets an appropriate priority; however, the achievability and measurement of this goal is not clear. While Horizon 2 outlines an aspirational end state, the absence of defined success metrics to compare against in 2028 creates uncertainty around how progress will be measured and when objectives can be considered achieved.

Furthermore, the centralisation efforts appear focused on the outcome of providing the levers necessary to protect the most critical assets, but this framing overlooks several other key benefits. A consistent, data-driven assurance model would provide greater visibility of risks and establish common baselines. A central capability would also reduce duplication efforts by

minimising fragmented, siloed risk and threat analysis undertaken independently across critical infrastructure operators. Rather than each entity repeating assessments in isolation, risks could be identified, contextualised centrally, and shared to inform sector-specific prioritisation and investment. This model would enable stronger analysis of risk trends, correlations, and behavioural patterns, supporting more targeted interventions and proactive risk management across the digital economy. If centralisation efforts are implemented and coordinated successfully, it is expected to better position the Australian government from a regulator to an enabler.

Recommendations

- Develop clear success metrics and a measurable end state.
    - Establishing concrete indicators would improve accountability, enable benchmarking, and provide a stronger basis for investment and policy decisions.
- Broaden the scope of risk centralisation beyond critical systems.
    - Centralisation should be leveraged not only to safeguard the most critical assets but also to identify systemic risks across sectors. A consistent, data-driven assurance model would reduce duplication of siloed risk analysis, provide clearer visibility of common risk drivers, and enable targeted interventions that strengthen resilience across the broader critical infrastructure ecosystem.
- Provide regulatory crosswalks to support private sector adoption of the SOCI act.
    - Regulatory crosswalks that map the SOCI Act requirements against other state, federal, industry and international frameworks such as the PSPF, ISM, NIST CSF and APRA CPS would help with private section adoption. It would allow critical infrastructure operators to direct more investment into practical security work by:
        - Reducing the complexity around compliance requirements.
        - Standards compliance implementation / reporting.
        - Minimising duplication of compliance efforts where obligations overlap, and
        - Easing compliance and audit fatigue.

Shield 6. Strong region and global leadership

"Driving a program of international regulatory alignment and enhancing regional cyber policy and regulatory capacity"

Significant progress has already been achieved under Horizon 1 in strengthening domestic supply chain security, particularly through regulatory reforms and critical infrastructure obligations. These foundations provide a strong platform for Australia to deepen its role as a trusted partner in global cyber resilience. However, supplier assurance remains highly fragmented across borders. Australian companies working internationally face a patchwork of different assurance framework. This creates duplication, inconsistency, and significant costs, especially for businesses embedded in global supply chains.

Given the increasing interdependencies of technology supply chains, an assurance framework that is interoperable across trusted partner is vital.

The Five Eyes community presents a natural platform for developing alignment, as it already operates with deep intelligence sharing and cyber cooperation. A harmonised supplier assurance approach would reduce barriers for Australian firms, improve the security of shared technology ecosystems, and send a strong signal internationally that compliance with partner nations' requirements can be trusted and reciprocal.

Recommendations

Adopt a Five Eyes-aligned supplier assurance framework that:

- Establishes a shared supplier vetting methodology across member states.
- Reduces duplication for Australian businesses engaged in cross-border procurement.
- Enhances confidence in international supply chains by ensuring assurance processes are consistent and trusted.
- Positions Australia as a secure and reliable partner of choice in the Indo-Pacific by championing interoperable assurance standards and leading regional collaboration on supplier risk management.

"Continuing to shape, uphold and defend international cyber rules norms and standards in our interests"

A solid foundation has been built through frameworks such as the Information Security Manual (ISM) and the Essential Eight, which provide important foundations for building cyber resilience. However, these exist within a fragmented international landscape. Organisations that operate across borders face overlapping obligations under different frameworks, such as National Institute of Standards and Technology (NIST), New Zealand Information Security Manual (NZISM), and others maintained by Five Eyes partners. The lack of consistent language and control mapping across these frameworks drives duplicated compliance efforts, higher costs, and assurance outputs that cannot be easily reused across jurisdictions.

Horizon 2 presents an opportunity for Australia to champion the alignment of these frameworks across Five Eyes partners. This would reduce the compliance overhead, improve trust in assurance processes, and ensure its domestic standards remain credible and internationally interoperable. The goal is not to replace national framework, but to create a translation layer so that assurance evidence against one framework (e.g., ISM) can be more readily recognised under another (e.g., NIST), and reciprocally the other way around.

Recommendations

Collaborate with Five Eyes partners to standardise governance frameworks by:

- Simplify internal mapping of principles, controls, strategies, standards to a common baseline / reference model.
- Developing regulatory crosswalks / cross-mapping tables across Five Eyes frameworks to harmonise language and controls.
- Agreeing on a core set of baseline controls that all partners recognise, with clear mapping to national variations.
- Promoting an international assurance template that enables entities to demonstrate compliance once, with evidence reusable across jurisdictions.