Classification: Public

MUFG Pension & Market Services

SUBMISSION TO DEPARTMENT OF HOME AFFAIRS
AUGUST 2025

Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

MUFG Pension & Market Services
A member of MUFG, a global financial group

1. EXECUTIVE SUMMARY

Who we are

MUFG Pension & Market Services, a member of the global financial group MUFG, is a global, digitally enabled business connecting millions of people with their assets. Through our two businesses, MUFG Retirement Solutions and MUFG Corporate Markets, we partner with a diversified portfolio of global clients to provide robust, efficient and scalable services, purpose-built solutions and modern technology platforms that deliver world class outcomes and experiences. Today our organisation has over 6,500 employees across the globe in 11 jurisdictions, working with some of the world's largest corporations, pension funds and financial institutions as our clients. Of these, more than half are Australian employees, located in offices in Sydney (CBD and Parramatta), Melbourne, Brisbane, Perth and Adelaide.

Link Market Services was founded in 2005 and listed on the Australian Securities Exchange (**ASX**) in 2015. In early 2024, it was acquired by Mitsubishi UFJ Trust & Banking Corporation (the Trust Bank, MUTB) and became MUFG Pension & Market Services. MUTB is the seventh largest bank in the world, with USD$3 trillion in assets, and is one of only 29 banks worldwide to be classified as a Global Systemically Important Bank (G-Sib), with world-leading risk management practices and centres of excellence in cybersecurity and fraud prevention.

We offer mission critical digital infrastructure in the geographies in which we operate. In Australia:

- MUFG Retirement Solutions provides administration services to 20% of the superannuation market.[1]
- MUFG Corporate Markets is a leading share registry, servicing 38% of the ASX 300.

We invest deeply in our technology, systems and processes to drive exceptional user experiences that leverage our people's expertise, combined with scalable technology, digital connectivity and data insights. Our systems are classified as critical infrastructure for the purposes of the *Security of Critical Infrastructure Act 2018* (Cth), which drives our significant ongoing investment in cybersecurity and operational resilience, protecting our clients as well as their members and/or shareholders.

Key Recommendations

As a critical infrastructure operator (**CI Operator**) for Australia's superannuation and financial markets sectors, our commentary and recommendations reflect our commitment to supporting a secure and resilient digital environment for the Australian economy. Our key recommendations are:

Recommendation 1: That the Government explores opportunities for **deeper integration of myID** with Australia's critical financial infrastructure.

Recommendation 2: That Government takes proactive steps to support PQC-readiness for CI Operators by:

- **issuing clear guidance and a national roadmap** for PQC-readiness across critical sectors**;**
- **providing access to scanning tools** to help identify systems and data flows that rely on vulnerable encryption methods**;**
- **offering targeted grants and funding to CI Operators** to support the assessment, planning and implementation of PQC-safe systems; and
- **investing in education and collaboration** initiatives that bring together government, industry and academic experts to raise awareness and accelerate secure, sector-wide implementation.

Recommendation 3:
To support businesses, particularly those safeguarding critical infrastructure, we recommend that the Government:

- **provides comprehensive guiding principles** for the safe adoption and use of AI;
- **issues clear recommendations on appropriate tooling**, including vetted AI safety and monitoring technologies suited to different industry sectors; and

[1] Measured by funds under management.

- **offers targeted grants** focused on building AI awareness, training and cyber capability uplift so that organisations can both harness AI's benefits and defend against its misuse.

Recommendation 4: That Government considers **requiring default MFA on email accounts** to address this critical vulnerability and enhance protection for both consumers and businesses.

Recommendation 5: That Government:

- **expedites the data retention legislative review** planned for Horizon 1 (initiative 9b) to provide greater clarity on data retention requirements for Australian businesses; and
- **implements a security-based exception to data sovereignty requirements based on Recital 49 of the UK and EU GDPR** to enable access to global cybersecurity services in a safe way.

Recommendation 6: That Government considers **introducing nationally consistent, mandatory testing standards for all CI Operators**, including tabletop exercises, business continuity testing, and control effectiveness assessments, to uplift preparedness and ensure a baseline level of cyber resilience across industries.

Recommendation 7: That Government should consider **expanding the current support** provided for top-tier CI Operators to all CI Operators.

Recommendation 8: That Government considers **undertaking an industry-wide review to develop benchmarks for security investment across critical infrastructure sectors**, taking into account organisation size, complexity and risk profile to help guide appropriate budgeting and ensure consistency in baseline cyber resilience.

2. DETAILED SUBMISSION

2.1. Outlook for Horizon 2: 2026-2028

As Australia moves into **Horizon 2 (2026–2028)** of its Cyber Security Strategy, two emergent technological developments are set to fundamentally reshape the threat landscape and merit immediate strategic attention from Government:

- **Artificial Intelligence (AI):**

  The rapid advancement and integration of AI into cyber operations – both defensive and offensive – will significantly alter the threat landscape. AI-enabled tools can enhance detection, response and threat intelligence through automation and predictive analytics. However, threat actors are also leveraging generative AI for more sophisticated phishing, social engineering and malware creation at scale. To stay ahead, Government must invest in secure AI development, support responsible AI use in cyber defence, assess the implications of AI-enabled threats on critical infrastructure and national security and support CI Operators with frameworks, tools and other support to navigate this shift.

- **Quantum Computing and Post-Quantum Cryptography (PQC):**

  While practical quantum computers capable of breaking current encryption standards are not yet widely available, their development is progressing rapidly. This poses a long-term but highly disruptive risk to the confidentiality and integrity of encrypted communications, financial systems and secure data storage.

  To prepare, Australia must accelerate efforts toward PQC readiness, including early adoption of quantum-safe algorithms, undertaking ecosystem-wide cryptographic audits, collaborating with international standards bodies and providing expert guidance and support to CI Operators to assist them to be PQC ready well ahead of 2030.

Horizon 2 presents a critical window to begin these transitions before quantum capabilities become real operational threats.

In our view, these stand out as demanding proactive engagement from government, industry and research sectors and are critical to shaping the nation's cyber posture and resilience. Specific recommendations in relation to these are provided in our commentary on ***Shield 2: Safe Technology*** below.

2.2. Specific recommendations and commentary

We provide commentary below on a number of specific areas raised in the Policy Discussion Paper, focusing on those most relevant to our operations and expertise. They are segmented under the relevant "Shields" and "Horizon 2 Focus Areas" as indicated in the Paper.

Shield 2: Safe technology

Horizon 2 Focus Area: Protect our most valuable datasets

Expanded use of Digital ID

We strongly endorse the Government's initiative to broaden the use of Digital ID in both public and private sectors. In the superannuation context, a trusted Digital ID system offers clear advantages in that it both:

- streamlines identity verification across onboarding, account access and major transactions, enhancing the member experience; and
- reduces the requirement to store and exchange large volumes of personal data, which in turn mitigates the risks of data breaches and identity crime.

As outlined in our recent whitepaper, Protecting Australia's Retirement Savings in a Digital World, we noted the intensifying cyber threat landscape targeting Australian superannuation. Globally, cybercrime is projected to cost US $10.5 trillion annually by 2025, while over 15 billion compromised credentials are currently circulating on the dark web. This has fuelled credential stuffing (where attackers test leaked username/password pairs to gain unauthorised access) which was behind the recent cybersecurity incident targeted at the superannuation industry in April 2025.

By reducing the repeated exchange and storage of sensitive identification data, Digital ID reduces the volume of high-value "honeypots" which attract threat actors, making member data fundamentally safer. MUFG Retirement Solutions is currently exploring verifiable credential solutions to both remove friction in the member experience and ensure data security, including significantly mitigating risks of credential stuffing.

Looking ahead, we encourage the Government to explore opportunities for deeper integration of its accredited Digital ID solution, ***myID***, with Australia's critical financial infrastructure. In the superannuation and financial markets sectors, enabling myID to serve as a verified and portable credential for member and investor identity could streamline onboarding processes and enhance fraud prevention across the ecosystem. This will both lift the baseline for identity assurance, as well as promote more effective interoperability between Government and private sector systems, supporting a more secure and frictionless digital economy.

Recommendation 1:

We recommend that the Government **explores opportunities for deeper integration of myID with Australia's critical financial infrastructure**.

Horizon 2 Focus Area: Promote the safe use of emerging technology

Quantum Computing and PQC readiness

As quantum computing capabilities advance, the security foundations of current cryptographic systems face an existential threat, particularly for CI Operators who rely on long-term data confidentiality. Threat actors are already

engaging in "*harvest now, decrypt later*" strategies, collecting encrypted data today with the expectation that quantum computing will render current encryption obsolete in the near future.

The Australian Signals Directorate (ASD) has signalled that critical infrastructure should be quantum-hardened by 2030. However, preparing for PQC is a complex transition likely to require a multi-year approach to implement. To maintain our resilience, it is imperative that we act today to ensure critical infrastructure systems are secure tomorrow.

In our view, CI Operators would benefit from guidance and education, access to scanning tools, as well as cross-industry collaboration to support each other to ensure Australia is PQC-ready. Targeted grants and funding would also ensure that small-medium providers can assess and upgrade their systems in line with national PQC-readiness goals, helping avoid gaps or delays across critical sectors.

Recommendation 2: In line with these developments, we recommend that the Government takes proactive steps to support PQC-readiness for CI Operators by:

- **issuing clear guidance and a national roadmap** for PQC-readiness across critical sectors;
- **providing access to scanning tools** to help identify systems and data flows that rely on vulnerable encryption methods;
- **offering targeted grants and funding** to CI Operators to support the assessment, planning and implementation of PQC-safe systems; and
- **investing in education and collaboration initiatives** that bring together government, industry and academic experts to raise awareness and accelerate secure, sector-wide implementation.

Artificial Intelligence in the context of cybersecurity

The advent of artificial intelligence will bring a seismic shift in how we work, with profound implications for Australia's cybersecurity posture. On the negative side:

- threat actors will be able to create highly sophisticated malicious code, automate attacks at machine speed and more easily evade existing controls;
- AI's propensity to hallucinate raises concerns about data integrity;
- widespread reliance on AI, especially unsupervised or poorly governed models, increases the risk of irreversible data leakage.

On the positive side, AI will be transformative – having the ability to power advanced detection systems capable of real-time identification of anomalies, automate threat-hunting across vast digital ecosystems, enhance predictive threat sharing and bolster resilience via self-learning defence mechanisms.

Businesses would benefit from Government support in the form of clear principles for safe AI use, recommended tools tailored to different sectors and targeted funding to build awareness, skills and cyber capability. We acknowledge the Government's work to develop a Voluntary AI Safety Standard, and consider this could be used as the basis for a more comprehensive set of principles, which include minimum AI standards for critical infrastructure operators, AI audit or oversight requirements, considerations for privacy impacts through AI adoption or use and their alignment with privacy reforms.

Recommendation 3: To support businesses, particularly those safeguarding critical infrastructure, we recommend that the Government:

- **provides comprehensive guiding principles** for the safe adoption and use of AI;
- **issues clear recommendations on appropriate tooling**, including vetted AI safety and monitoring technologies suited to different industry sectors; and
- **offers targeted grants** focused on building AI awareness, training and cyber capability uplift so that organisations can both harness AI's benefits and defend against its misuse.

Shield 3: World-class threat sharing and blocking

Horizon 2 Focus Area: Amplify existing government and industry models for threat blocking and threat sharing

Mandating MFA for email accounts

We believe that a key way in which the Government could support threat blocking is by mandating that email providers enable multi-factor authentication (MFA) by default.

While most providers offer MFA, its optional nature limits uptake by end users and mandating it by default would make a significant difference.

The recent credential-stuffing incident targeting superannuation funds involved threat actors leveraging compromised email accounts to perform password resets and gain access to funds. Had MFA been enforced on email accounts by default, this attack vector would have been far less effective, as attackers could not have bypassed second-factor checks even with the stolen credentials.

Recommendation 4:

We recommend that the Government considers **requiring default MFA on email accounts** to address this critical vulnerability and enhance protection for both consumers and businesses.

Data retention and data sovereignty

The Horizon 1 initiative to review Commonwealth data retention legislation (see Initiative 9b in Appendix B to the Paper) remains "in progress," with completion expected by the end of 2025. Given that we are now approaching Q4 2025, it is possible that this completion date may be at risk.

We note that the absence of updated guidance creates uncertainty for businesses seeking to comply with overlapping data retention, privacy, and cybersecurity obligations, particularly where those businesses operate in regulated or high-risk sectors. Clear and practical guidance on the type of data required to be retained, for how long and under what conditions is needed. Clearer privacy requirements might have enabled organisations to better manage aged or legacy data, potentially mitigating the impact of several recent high-profile security incidents in Australia. Accordingly, we urge the Government to prioritise this review.

In addition, we consider that there is a need for clearer guidance on data sovereignty requirements, particularly in respect of the use of global infrastructure for cybersecurity purposes. Under the *Privacy Act 1988* (Cth), personal information may be disclosed to an overseas recipient only if the disclosing entity takes reasonable steps to ensure that the recipient does not breach the Australian Privacy Principles (APPs), or if an exception applies – such as where the recipient is subject to a law or binding scheme that offers substantially similar privacy protections, or where the individual has given informed consent. This can create challenges for the many organisations that need to leverage global cybersecurity resources, such as threat intelligence or managed detection and response services, which may not be available from providers in countries with adequate privacy protections.

Accordingly, we consider that the Government should look at implementing a targeted carve-out which permits cross-border data transfers where it is necessary for network and information security and adopt Recital 49 of the UK's General Data Protection Regulation (GDPR) (based on the EU's GDPR) as a model. Recital 49 creates a narrow exception to permit cross-border personal data processing to the extent "strictly necessary" for the purposes of network and information security.

Adopting a similar carve-out in Australia would enable organisations to access vital global cybersecurity services, improving national cyber resilience without compromising data safety or privacy. Currently, the absence of a similar security-based exemption may hinder Australia's ability to respond effectively to evolving cyber threats.

Recommendation 5:

We recommend that the Government:

- **expedites the data retention legislative review** planned for Horizon 1 (initiative 9b) to provide greater clarity on data retention requirements for Australian businesses; and
- **implements a security-based exception to data sovereignty requirements based on Recital 49 of the UK and EU GDPR** to enable access to global cybersecurity services in a safe way.

Shield 4: Protected Critical Infrastructure

Horizon 2 Focus Area: Strengthen cybersecurity obligations and compliance for critical infrastructure

Strengthen testing requirements for CI Operators

Currently the SOCI Act imposes mandatory testing and preparedness obligations on CI Operators. In addition, there may be requirements imposed by regulators in specific industries – for example, APRA's prudential standards CPS230 (Operational Risk Management) and CPS 234 (Information Security). While regulators may issue guidance under the standards, there is no consistent, mandated testing framework across all critical infrastructure.

To address this gap, we recommend expanding and mandating a set of core cybersecurity and operational resilience testing practices for all CI Operators. These should include:

- **Cybersecurity tabletop exercises** to test incident response plans in simulated real-world scenarios, helping teams coordinate and identify gaps in crisis handling.
- **Business continuity and resilience exercises** to ensure organisations can maintain essential services during disruption and recover quickly from cyber incidents.
- **Control effectiveness testing** (e.g., penetration testing or red teaming) to validate that security controls are functioning as intended and can withstand real-world attack techniques.

Given the critical role these systems play in the Australian economy and national security, applying consistent, robust testing requirements across all sectors is essential. This would also provide certainty to CI Operators and their clients and customers that certain minimum standards of testing are being met.

Recommendation 6:

We recommend that Government considers **introducing nationally consistent, mandatory testing standards** for all CI Operators, including tabletop exercises, business continuity testing, and control effectiveness assessments, to uplift preparedness and ensure a baseline level of cyber resilience across industries.

Greater support for CI Operators

After expanding the definition of critical infrastructure in 2022, the Government's support and regulatory focus has largely centred on larger infrastructure providers, such as telecommunications companies and major utilities.

However, the broader set of CI Operators, including smaller to medium providers or regionally based providers, play an equally important role in Australia's national resilience. These organisations face similar cyber threats and operational risks as larger providers and would benefit from more targeted support to enhance their existing capabilities and sustain strong security practices over time.

For example, we understand that the Government already facilitates wide-ranging support for top-tier CI Operators, including running tabletop exercises and hosting educational events. Extending these activities to include all CI Operators would provide broader benefits and strengthen resilience across the sector.

Recommendation 7:

The Government should consider **expanding the current support** for top-tier CI Operators to all CI Operators.

Provide guidelines/benchmarking for appropriate security investment for critical infrastructure

As cyber threats grow in sophistication and frequency, it is essential that CI Operators are resourced to maintain effective and proportionate security controls. An industry-wide view of security investment benchmarks based on sector, size and risk profile would be a valuable tool to support strategic planning and ensure alignment with best practices. This could help organisations better validate their current investment levels at an individual level, as well as collectively contributing to more consistent resilience across sectors.

Recommendation 8:

We recommend that Government considers **undertaking an industry-wide review to develop benchmarks for security investment across critical infrastructure sectors**, taking into account organisation size, complexity and risk profile to help guide appropriate budgeting and ensure consistency in baseline cyber resilience.

Other comments – Supporting Small to Medium Enterprises

While we did not provide specific commentary on Shield 1 (Stronger Businesses and Citizens), we consider that Government could consider applying some of the suggestions and recommendations made above to small to medium enterprises (SMEs), such as:

- Providing SMEs with greater access to affordable advice to deal safely with emerging technological developments such as quantum computing and AI;
- Offering targeted grants to support their cybersecurity capability uplift and sustainment of security oversight and controls; and
- Expanding the Cyber Hygiene Improvement Programs (CHIPs) to small-medium enterprises, to support identification of vulnerabilities and to provide advice or support with addressing them.

3. CONCLUSION

MUFG Pension & Market Services appreciates the opportunity to contribute to this consultation and welcomes continued engagement with the Department of Home Affairs regarding its consultation into Horizon 2 of its Cyber Strategy. We would further welcome the opportunity to meet with you to discuss the detail of this submission or any other relevant matters.

To arrange a meeting, please contact [redacted]