FORESCOUT

Forescout Submission to Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

29 August, 2025

FORESCOUT

Forescout Submission to Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Overview

This paper is Forescout Technologies' response to the Department of Home Affairs' Horizon 2 Cyber Security Policy Consultation Paper (August 2025). It provides observations on the evolving cybersecurity landscape and practical considerations for implementing the policy directions outlined in the consultation.

Drawing on more than two decades of operational experience supporting governments, defence, and critical infrastructure organisations, Forescout offers insights into areas where continuous visibility, Zero Trust adoption, and automated controls can strengthen resilience at scale. The response is structured to align with the consultation themes, contributing constructively to policy development, and ensuring proposals are both practical and achievable in the Australian context.

Forescout's comments in this submission include our views on:

- The Gaps in implementing Horizon 1. Priority activities that require urgent implementation to establish a solid foundation for Horizon 2.
- Hastening the implementation of Zero Trust
- Horizon 2 Shield 2, Safe Technology – Part 1 Quantum Safe
- Horizon 2 Shield 2, Safe Technology – Part 1 Operational Technology

About Forescout

In an era when adversaries exploit the interconnectedness of our democratic societies, Forescout Technologies stands not just as another tech vendor, but as an operational partner that federal entities trust to reduce the probability and impact of significant cyberattacks. With over two decades of operational experience, Forescout has earned the confidence of Fortune 100 companies and governments with complex systems that can not go down. Our strength lies in delivering automated cybersecurity at scale, covering every device across IT, operational technology (OT), the Internet of Things (IoT), and medical technology (IoMT). Forescout exposes vulnerabilities, enforces compliance, and reduces the attack surface through automated segmentation and policy enforcement.

Forescout translates Zero Trust from principle into practice. Through its 4D Platform™, every device, user, and interaction is continuously authenticated and validated. This dynamic model replaces static perimeter defenses with adaptive, risk-based controls that respond in real-time. What sets Forescout apart is its ability to extend Zero Trust to unmanaged, mission-critical, and OT assets. By enforcing least-privilege access and embedding continuous trust evaluation, it reduces lateral movement, contains breaches, and ensures missions continue even under sustained attack.

Vedere Labs adds further depth. More than a decade of research has exposed vulnerabilities and attack patterns across IT, IoT, OT, and medical devices. Drawing on a global sensor network and adversary simulations, Vedere Labs tracks threats in real-time and produces actionable insights. Its Global Cyber Intelligence Dashboard, aggregating over 39 billion data points, provides governments with a unique vantage point on risks and vulnerabilities. For Australia, this strengthens early warning and guides mitigation strategies.

FORESCOUT

The Gaps in Implementing Horizon 1 – Policy Not Yielding Results

Area Where Urgency Is a Priority - Government

In Horizon 1, Shield 4, Uplifting cyber security of the Commonwealth Government, the Strategy said:

> *To provide ongoing accountability, we will develop an internal cybersecurity program and assurance function. We will scale up support to government entities, uplifting their maturity against the Essential Eight. We will also conduct regular reviews of the cyber maturity of Commonwealth entities, as part of the Investment Oversight Framework, led by the Digital Transformation Agency. These reviews will inform further evolution of our security frameworks and help government entities meet changes in the evolving threat landscape.*[1]

Many government agencies remain below Maturity Level 2, and uptake of cybersecurity tools has been uneven. While frameworks and assessments have proliferated, implementation has lagged. Government continues to face challenges in translating policy into operational resilience, often due to constrained funding, limited access to scalable solutions, and uncertainty as to where to invest scarce funding.

The Australian Signals Directorate and the Australian Cyber Security Centre's report of Commonwealth Cyber Security Posture in 2024, which informs the Parliament, surveyed and obtained responses from 94% of 190 Australian Government entities. It revealed that government entities are going backwards. Despite numerous reviews and maturity assessments, most agencies have not progressed beyond Level 1 and have, in fact, declined.[2] It's survey found:

> *"The proportion of government entities that reached maturity level 2 across the Essential Eight mitigation strategies has declined. In 2024, 15 per cent of all entities reached overall maturity level 2, decreasing from 25% in 2023.*

It is clear from this result that the actions from Horizon 1 are not delivering results, and there is a concerning cybersecurity risk of threats to the Australian Government's national infrastructure that Australians rely on every day.

Fund the Foundations While Concurrently Expanding into the Horizon 2

Forescout is noticing a lack of urgency in agencies to improve their cybersecurity posture. Despite growing awareness of cyber threats, many government agencies remain stalled in their cybersecurity journey, not due to reluctance but due to uncertainty. The challenge is not resistance to change, but a lack of clarity on how to proceed and a fear of missteps in an unforgiving threat environment. In effect, agencies are being asked to lead without a map. The absence of clear exemplar agencies that model best practice and demonstrate successful implementation has created a vacuum.

As the saying goes, "you can't be what you can't see." Without visible leadership and coordinated guidance, progress will remain fragmented, and risk exposure will deepen.

This is a call to arms: Government must not only set policy ambition but also illuminate the path forward. Agencies need practical frameworks, shared success stories, and targeted investment to build confidence and capability. Leadership must be visible, actionable, and funded.

---

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf, page 43.

[2] The Commonwealth Cyber Security Posture in 2024, Australian Cyber Security Centre https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2024.

Importantly, the Government must make sure funding is available, so agencies aren't making trade-off decisions about where they spend their limited funds.

Forescout recommends:

1. Showcase agencies that are demonstrating high maturity levels and use independent data to demonstrate how they are performing.
2. Governments recognise that assessments of what good looks like need to be more independent, with agencies not doing their own assessments, with the potential of them being 'light' on themselves. They need to utilise effective tools that are available to demonstrate where they are performing and where they have weaknesses that make their networks vulnerable, and show it in real or near real time.
3. Improve the Digital Transformation Agency Investment Oversight Framework reviews so there is greater transparency about how agencies are performing in improving their cybersecurity posture and maturity. Use the independent performance data from 2 and release the information publicly.
4. Address the underinvestment in cyber security across government agencies, so the Government provides targeted funding to address the key weaknesses.
5. As funding rolls out and builds exemplar agencies across portfolios, continue to showcase their efforts towards building an increasingly cyber resilient public service.
6. Support key critical infrastructure industries to build exemplar models that others can follow.

Hastening the Implementation of Zero Trust

The Australian Government's Cyber Security Strategy 2023–2030 rightly identifies Zero Trust as a foundational principle for securing public sector systems, and we commend its integration into the Protective Security Policy Framework (PSPF) as a signal of serious intent. Zero Trust is now widely accepted as the way forward, reflecting global best practice in mitigating identity-based threats and lateral movement across networks. However, implementation remains uneven, with agencies facing barriers such as legacy infrastructure, fragmented identity management, and limited funding for sustained transformation. It is also not clear that there is industry and government adoption of the necessary requirements to deliver Zero Trust.

Forescout recommends:

1. The Government formally adopts NIST SP 1800-35 "Implementing Zero Trust Architecture" as the leading implementation guide for Zero Trust.
2. Provide new funding to support whole-of-government adoption of the Zero Trust principles in the PSPF at scale.
3. Invest in exemplar agencies that can demonstrate practical, scalable models of Zero Trust in action—thereby fostering capability uplift and cross-agency learning.

FORESCOUT

Horizon 2 Shield 2: Safe technology

Part 1. Quantum-Safe

Quantum Computing and Australia's Cybersecurity Readiness

Quantum computing is no longer a distant frontier; it is rapidly approaching operational reality. Recent industry surveys suggest commercial quantum applications may emerge as early as 2026. This shift demands urgent attention from policymakers, as quantum capabilities pose a direct threat to the cryptographic foundations of Australia's digital infrastructure.

Quantum machines will be capable of solving complex problems at speeds exponentially faster than classical computers. This leap in capability undermines current encryption standards, particularly public key infrastructure (PKI), which secures the vast majority of government, defence, and commercial communications. Once quantum computers reach sufficient scale, they will be able to break widely used encryption protocols, placing sensitive data at risk, including diplomatic cables, military intelligence, and proprietary corporate information.

Importantly, the threat is not limited to future data. Information harvested today may be decrypted in years to come, compromising long-term confidentiality ('harvest now, decrypt later'). Australia must act now to ensure our systems, standards, and sovereign capabilities are prepared for the quantum era.

Forescout has identified the issues and has published articles on the dangers of quantum to cybersecurity. Below are some links to a more detailed analysis of the problems and solutions that Quantum computing imposes on our cybersecurity resilience.

Forescout recommends:

1. **Establish a National Quantum Risk Framework and Roadmap.** (The approach undertaken by the Department of Homeland Security in the United States is worth considering).[3] Use this to develop a coordinated strategy across government, defence, and industry to assess quantum vulnerabilities, prioritise critical assets, and guide mitigation efforts.
2. **Accelerate Post-Quantum Cryptography Adoption.** Mandate the transition to quantum-safe algorithms in government systems and critical infrastructure, aligned with international standards, including those recommended by NIST.
3. **Invest in Sovereign Capability for Quantum-Safe Technologies.** Support Australian research and commercial development of post-quantum cryptographic tools, secure key exchange platforms, and detection systems to reduce reliance on foreign technologies.
4. **Launch a National Transition and Awareness Program** to provide guidance and funding for industry and community education on quantum risks, and support the migration of legacy systems, particularly those with long data retention cycles, to quantum-resilient standards.

Quantum computing will reshape the digital landscape. Australia must lead with foresight, ensuring our cybersecurity posture remains robust, adaptive, and sovereign in the face of emerging threats.

[3] https://www.dhs.gov/quantum

The following links from Forescout provide more information about the need for post-quantum cryptography:

1. The Future of Encryption in a Quantum Cryptology World. This article explains quantum and the benefits of moving on Post-Quantum Cryptography.
2. Post Quantum Crytography: The Real Risk of Not Adopting It. This article explains the data on current progress to Post- Quantum Cryptography.

Unfolding Shield 2 – Part 2 Operational Technology

While the Internet of Things was well covered in Horizon 1, Horizon 2 needs to turn to Operational Technology, which includes devices that are functionally specific with a clear function or role. Many of these devices are vulnerable to damage from intrusion, information being harvested, potential tampering with the device function, or providing access to broader systems. All create risks to infrastructure and people.

OT security is challenging because these systems were never designed to face cyber threats, yet they are increasingly connected and targeted. The biggest risks come from legacy vulnerabilities, IT/OT convergence, lack of visibility, and the high stakes of downtime or safety incidents.

Forescout's Recommendations for Securing OT

Establish mandatory, automated asset visibility and control across OT environments. Australia cannot defend what it cannot see. While asset registers exist today, they are often static, incomplete, or reliant on manual reporting. Horizon 2 should mandate the deployment of automated asset discovery and continuous monitoring capabilities across critical OT environments. This will allow operators and the government to maintain a real-time understanding of what is connected, what is vulnerable, and what must be defended, as resilience must be grounded in facts, not assumptions.

Require dependency mapping that extends beyond compliance to operational resilience. The Security of Critical Infrastructure Act 2018 (SOCI Act) framework already requires operators to identify critical dependencies, but in practice, this remains a paper exercise. Horizon 2 provides an opportunity to go further: embedding dynamic dependency mapping that accounts for supply chains, system interdependencies, and real-world operational constraints. This would move the conversation from theoretical compliance to practical resilience, ensuring that when one node is compromised, the larger system does not fail.

Specific steps include:

1. **Achieve Full Visibility and Continuous Asset Discovery**
   - It is vital to identify, classify, and continuously monitor all OT assets, including those traditionally hidden, unmanaged, or unagentable, without disrupting operations. Visibility underpins every other security control. (Fortinet, SecurityBrief New Zealand, Forescout)

2. **Prioritize Risk Using Asset Intelligence**
   - Using an Asset Risk Framework assigns both Cybersecurity Risk and Operational Risk scores, enabling organisations to triage assets and focus on the most critical vulnerabilities. (Forescout, Australian Cyber Security Magazine)
   - This dual scoring helps balance safety, uptime, and security decisions, especially where patching or downtime may not be feasible.

3. Detect Threats Through Non-disruptive Monitoring

- With OT devices needing to be continuously operational, passive network monitoring and anomaly detection are central to early threat detection in OT environments, avoiding disruptions from active scanning. (Medium, Forescout)
- Real-time dashboards and industrial threat libraries enhance situational awareness for both SOC and OT teams. (Forescout, Keysight)

4. Automate Response and Orchestration

- Automation is key to enabling orchestrated controls, including network segmentation and incident response, minimising manual intervention, and managing operational risk. (Forescout, SecurityBrief New Zealand)
- Using a security platform that supports seamless integration with broader IT and OT ecosystems, enabling workflows that bridge security and operational teams. (Forescout)

5. Support Hybrid Deployments Across IT, OT, IoT/IoMT

- Use an OT security platform that is designed to adapt to various architectural patterns, including air-gapped, cloud-based, or hybrid OT environments. (Forescout, Cybersecurity Excellence Awards)
- Security platforms that support a large number of industrial protocols (up to 350) and a wide range of passive and active discovery techniques. (Forescout, Cybersecurity Excellence Awards)

6. Align with Cybersecurity Frameworks and Compliance

- Solutions that support key industry frameworks like IEC 62443, NIST CSF, NERC CIP, ISO 27001, and more for native compliance and reporting. (Forescout, Australian Cyber Security Magazine)
- They help automate compliance workflows and provide actionable audit trails across OT environments.

7. Workforce & Culture

- Ensure there is specialised OT security training for operators, engineers, and IT staff.
    - Idaho National Lab's Cyber Informed Engineering development tools are a great place to start.
- Encourage cross-team collaboration so IT and OT teams must work together (avoid silos).
- Insider threat awareness: Monitoring and access control for staff and contractors.

Forescout recommends that visibility is the essential first step; you can't secure what you can't see, and encourages organisations to build a bridged OT-IT security strategy. Automation and risk-based analytics are vital for reducing manual workload and improving resiliency without sacrificing operational continuity.

Forescout recommends the Government:

1. Empower and appropriately fund the Critical Infrastructure Security Centre (CISC) to lead the implementation of Horizon 2 OT-IT security integration strategies across critical infrastructure sectors, utilising best practice as listed above. Through the Risk Management Program, CISC should engage with entities and government agencies, including regulators, to ensure the development and adoption of bridged OT-IT security strategies, supported by robust reporting frameworks to boards and executive leadership.
2. Require entities to formally attest, via mechanisms coordinated by CISC, that they have established and operationalized the above strategies and suitable governance frameworks and reporting structures. These should demonstrate clear oversight of OT-IT security integration and provide regular assurance to leadership teams and boards on progress and risk posture.
3. Expand the remit of the Critical Infrastructure Security Centre (CISC) to include targeted capability uplift programs for OT-IT security integration, with a focus on sovereign data handling, local workforce development, and sector-specific risk mitigation. This should be supported by sustained investment and policy alignment, with the support of regulators, to ensure that critical infrastructure entities can access trusted guidance, tools, and training tailored to their operational environments.
4. Work with the Tertiary Education Quality and Standards Agency (TEQSA) and universities and colleges to ensure every student pursuing a degree in engineering also completes coursework in cybersecurity and its impact on the industrial setting. Idaho National Lab's **Cyber Informed Engineering development tools** should be used as a baseline.

FORESCOUT®

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com