

Submission on the Five Pillars Interim Reports

Dear Commissioners,

Thank you for the opportunity to contribute to the Five Pillars inquiries. The interim reports set out an ambitious reform agenda across the systems that shape Australia's productivity. Cybersecurity and the security of operational technology (OT) are the digital foundations that support all five pillars. They safeguard national security and enable economic growth, underpinning long-term productivity. Their strength will determine whether systemic reforms can scale, confidence can be sustained, and growth is delivered in practice.

The Commission's emphasis on systems thinking is well founded and clearly articulated. Digital security should be framed not as an isolated risk, but as an integrated capability that shapes outcomes across systems. This is acknowledged most clearly in the data and digital pillar, where strong security and privacy frameworks are recognised as essential for the adoption of AI, digital reporting, and new data-access models¹. That emphasis on trust is warranted.

The picture is less complete across the other pillars, where reforms hinge on highly digitised and operational systems. In energy, productivity gains from distributed renewables, storage, and smart grids depend on the integrity of critical systems. Recent outages linked to OT compromise show how quickly output can contract and investor trust can erode. When ports or grids are offline, the cost is not just in repairs but in lost exports, idle supply chains, and higher insurance premiums. The 2023 DP World cyber incident, which temporarily halted around 40% of Australia's freight trade, demonstrates the scale of these impacts².

These disruptions also expose national security vulnerabilities, as highly digitised sectors such as energy, transport and manufacturing are integral to both economic performance and strategic resilience. The Government's Future Made in Australia agenda and its National Interest Framework recognise industrial capability, clean energy manufacturing and critical minerals processing as strategic priorities. To realise these ambitions, cybersecurity, particularly for OT and critical system integrity in manufacturing, must be explicitly integrated to safeguard both productivity and national security.

In healthcare, digital security underpins efficiency and public trust. Systems depend on integrated data, connected devices, and the contracting of services across multiple providers. Breaches in health systems demonstrate how fragile this foundation can be. The Medibank breach alone created direct costs of over A\$46 million with projected total costs exceeding \$125 million, while hospital ransomware incidents have forced the cancellation of hundreds of procedures³. These are not marginal risks; downtime is a direct economic drag that compounds across sectors.

The dynamic economy pillar also reveals the same dependency. Resilient growth through innovation and business investment depends on market confidence that digital and operational systems are reliable. Streamlined regulatory approaches that reduce duplication and compliance costs further encourage participation and support adoption⁴. Unless cyber security and OT security are integrated into reforms across all pillars, reforms may fall short of their full productivity potential.

¹ Productivity Commission (2024), Harnessing Data and Digital Technology Interim Report; <https://www.pc.gov.au/inquiries/current/data-digital/interim>

² DP World Australia (2023), Port Cyber Incident

³ Medibank Private Limited (2023), FY23 Half Year Results: Cyber Incident Update

⁴ Productivity Commission (2024), Creating a More Dynamic and Resilient Economy Interim Report; <https://www.pc.gov.au/inquiries/current/resilient-economy/interim>

The workforce pillar highlights the scale of the challenge. Adaptability and mobility are rightly prioritised, yet cybersecurity capability exposes a deeper fragility of the workforce system. Australia faces a projected shortage of around 3,000 professionals by 2026⁵, within that workforce, dedicated cybersecurity professionals remain a small cohort. AustCyber estimated 51,000 in dedicated roles in 2022, with only 11,000 in specialist functions such as penetration testing, security architecture and incident response⁶. Attrition and mid-career leakage, particularly the loss of women from the field, further compound the challenge⁷. The cyber workforce case illustrates the broader importance of treating capability as evolving human capital critical to productivity outcomes. Adaptability must be framed as capability building that evolves with demand, not as a fixed stock of skills to be managed. If left unaddressed, this shortfall will constrain not only digital adoption, but the broader reforms needed to lift productivity.

The evidence underscores the point. Based on official business counts and Australian Cyber Security Centre loss data, even a conservative estimate places annual small business cybercrime losses at over \$12.8 billion⁸⁹. This underscores cybercrime as a direct and growing drag on national productivity, eroding public confidence in the security and value of digital systems. By contrast, resilient organisations recover output up to 40% faster than peers, demonstrating the productivity dividend of investment in security. Organisations that invest in resilience are less likely to be impacted by opportunistic intrusions, reducing both the frequency and severity of disruption. This is not only a security benefit but an economic one: fewer incidents, lower compliance and recovery costs, and stronger investor trust. Productivity is strengthened when businesses treat cybersecurity as capital investment, not regulatory burden, and when government create the conditions that make resilience an asset for growth.

This approach is consistent with the Australian Cyber Security Strategy 2030, which recognises cybersecurity as both an area of national security risk and a driver of economic fortitude. The Strategy further highlights the role of regulatory simplification, secure technology adoption, and critical infrastructure resilience. These national reforms provide the security baseline, while the Commission's task is to ensure that productivity reforms are designed to capture the economic benefits enabled by secure digital foundations.

Fortinet can actively support the Productivity Commission's reform agenda by contributing data, analysis, and global experience. Drawing on our global threat intelligence, also used to drive key partnerships with the World Economic Forum's Centre for Cybersecurity, the Cybercrime Atlas initiative, INTERPOL Gateway, and the Cyber Threat Alliance, we provide forward-looking visibility of risks to critical systems, helping policymakers calibrate focus on reform pathway options. Through the Fortinet Training Institute, we are addressing workforce shortages by equipping students and professionals with industry-recognised certifications and practical pathways, delivered in collaboration with universities, TAFEs, and schools worldwide. Our global experience in securing essential infrastructure offers evidence-based insights to reduce investment risk and sustain productivity growth.

⁵ AustCyber and Australian Signals Directorate projections on cyber workforce shortages. <https://www.cyber.gov.au>

⁶ AustCyber (2022), Cyber Security Sector Competitiveness Plan; ACS workforce analysis, https://cdn.stoneandchalk.com.au/australias_cyber_security_sector_competitiveness_plan_2022_3_92136dca99.pdf

⁷ Australian Women in Security Network (2023), Gender Dimensions of the Security Sector in Australia Study <https://www.awsn.org.au/resources/gender-dimensions-of-the-security-sector-in-australia-study/>

⁸ Australian Bureau of Statistics (ABS) 2024, *Counts of Australian Businesses, including Entries and Exits, June 2019 to June 2024*, cat. no. 8165.0, Canberra.

⁹ ACSC Annual Cyber Threat Report: nearly half of Australians online report being victims of cybercrime annually. Available at: <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024>

Our recommendations demonstrate how security can be embedded into existing reforms in ways that build market support, deliver resilience dividends, and accelerate technology adoption. We stand ready to contribute these capabilities to help ensure reforms are resilient, trusted, and delivered at scale. We would welcome the opportunity to provide further case evidence on OT resilience, cybersecurity workforce pathways, and productivity-oriented investment models to assist the Commission in shaping practical, durable recommendations. These insights are not about compliance obligations or red tape, but about ensuring that reforms deliver productivity gains in practice.

Recommendations

We agree a growth mindset is essential. In preparing this submission, Fortinet has considered the Commission's draft recommendations across all five pillars. The following recommendations seek to strengthen Australia's digital security and enhance productivity.

- The Commission recommends stronger incentives for business investment. Recognising cybersecurity and OT security investment as productivity-enhancing capital would align directly with the Commission's agenda to lift business investment, reframing security from compliance overhead to capital formation, driving multifactor productivity by protecting continuity of output and lowering risk premiums for investors.
- The data and digital technology pillar recognised the need for innovation-friendly privacy regulation and improved data access. Digital security is the trust enabler that allows these reforms to scale. Without it, the benefits of AI, reporting reforms, and new data sharing models cannot be realised. Support ongoing regulatory streamlining led by Home Affairs. Reducing duplicative compliance pathways lowers transaction costs, encourages small to medium businesses participation, and accelerates the adoption of secure digital systems.
- Energy, care, and infrastructure depend on connected systems that rely on confidence that sensitive data and connected devices are secure. Incorporating baseline security requirements into approvals and contracting processes ensures productivity gains are sustainable in practice. Incorporating OT security standards into these processes would safeguard infrastructure, de-risk capital, and ensure productivity gains are sustainable.
- The Commission highlights the need for flexibility and new pathways in the skilled and adaptable workforce pillar. The cybersecurity domain exemplifies this challenge, with acute shortages and fragile retention. Embedding cybersecurity capability into reskilling and retention strategies for priority sectors would operationalise the Commission's recommendations in a sector critical to all others.



Nicole Henry
Head of Government Affairs ANZ
Fortinet