Submission for Horizon 2 of the 2023-2030 Australian Cyber Security Strategy:
Detailed Recommendations for a National Innovation & Commercialisation Chapter

Presented by UBIQ Ventures to the Australian Cyber Security Strategy Team, Department of Home Affairs
28 August, 2025

1. Executive Summary: A Proposal to Catalyse a Sovereign Cyber Security Innovation Ecosystem

I. The Challenge: A Critical Investment Gap

Australia faces a significant market failure in the commercialisation of its cyber security innovation. Despite world-class research, only 0.7% (AUD $29M) of Australian venture capital was invested in early-stage cyber security companies in 2024. This pales in comparison to global innovation hubs like Israel, which attracted $3.8 billion in the same period. This underinvestment hinders our ability to develop sovereign capabilities, forcing reliance on foreign technology and leaving a significant economic and national security opportunity untapped. To achieve the 2030 vision of being a world leader, Australia must transition from a technology consumer to a technology producer.

II. The Solution: An Innovation & Commercialisation Chapter

We propose the introduction of a dedicated, cross-cutting **Innovation & Commercialisation Chapter** within Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. This chapter would focus on deploying practical, non-legislative mechanisms to catalyse private investment and build the permanent infrastructure needed for a self-sustaining innovation ecosystem.

III. Proposed Initiatives: A Five-Point Plan for Action

We propose six synergistic initiatives, based on the success of similar programs elsewhere and adjusted to what UBIQ has analysed as the core needs to build a thriving Australian cyber security startup ecosystem. Each can be deployed individually or in combination using existing government mechanisms, without new legislation or bureaucracy:

- **Cyber Security Venture Capital Co-Investment Fund:** A bold, $100M balance sheet investment, modelled on the successful Biomedical Translation Fund (BTF), to act as a cornerstone investor in specialised, private-sector cyber security VC funds.
- **Targeted VC Co-Investment Programme:** An agile alternative to the large-scale fund. The government would invest $8M into each of up to three specialised cyber security VCs, conditional on them raising at least $30M in private capital, creating a significant multiplier effect with a smaller government footprint.
- **Direct Investment & Investor Incentives:** A more granular program to de-risk private capital through an enhanced ESVCLP incentive for fund investors and a

direct co-investment grant for early-stage companies.

- **National Cyber Security Accelerator Programme:** A $22M grant program to establish up to two world-class cyber security accelerators, building the "factory floor" for new sovereign companies.
- **Venture Fund Establishment Grants:** A $1.75M grant program to lower the barriers to entry for up to three new, specialised cyber security VC funds, growing local expertise.
- **Prioritising R&D Commercialisation Pathways:** A program to create dedicated cyber security streams within existing, successful R&D commercialisation vehicles like the BRII and ARC linkage grants.

IV. Recommendation and The Path Forward

To ensure immediate impact, we recommend a high-priority package including the **National Cyber Security Accelerator Programme** and **Venture Fund Establishment Grants** (totaling ~$24M) as essential ecosystem infrastructure. This must be paired with a significant capital stimulus, for which we recommend the agile and highly-leveraged **Targeted VC Co-Investment Programme** (additional ~26M).

In a nascent sector of national importance, the Australian investment community looks to the government to lead. This targeted intervention is the catalyst required to de-risk the sector, unlock significant private capital, and build a world-class, sovereign cyber security industry.

This document provides a high-level overview of our detailed submission. UBIQ Ventures is ready and happy to present, discuss, and assist in any aspect of this proposal.

2. Introduction: About UBIQ Ventures & Our Founders

UBIQ Ventures is the first and only cyber security-focused, early-stage venture fund in Australia, operating as a hands-on venture creation foundry. Unlike traditional venture capital funds, we actively ideate, originate and co-found companies to address identified gaps in the global cyber security market. Our model combines the velocity and execution of Israel's startup DNA with the scaling advantages of the US market, providing our portfolio companies with a competitive edge from day one.

UBIQ is led by a unique blend of Australian-American-Israeli operators located in both Australia and the US, with proven global experience in cyber security, venture building and scaling companies from pre-seed to exit. The founding team includes Ami Hofman, a former CISO with over 30 years of C-level cyber security leadership and deep connections across the APAC ecosystem; Ariel Cohen, who brings extensive US and Israeli startup go-to-market expertise, having built global teams for two startups from pre-seed to exit and served as a global technology partnerships lead at Palo Alto Networks after over a decade in Israel's Unit 8200. Recognised by the Australian Government's Global Talent Program for his expertise in cyber security, Ariel has relocated to Australia to help build the nation's sovereign cyber capabilities; and Warren Small, a global innovation leader formerly with NTT Ltd, with a track record of leading incubation and GTM efforts across the US, Australia and South Africa.

We are currently in the setup and fundraising stage for our AUD $45M Fund I and plan to commence operations in the beginning of 2026. Our unique position provides us with a frontline view of the challenges and immense potential within Australia's sovereign cyber ecosystem. This submission is informed by our direct experience in building globally competitive companies from an Australian base and our commitment to helping achieve the 2030 vision outlined in the National Cyber Security Strategy.

3. The Critical Investment Gap in Australian Cyber Security

We commend the Australian Government on the visionary approach and significant progress made under Horizon 1 of the 2023-2030 Australian Cyber Security Strategy. The foundational work has been critical in strengthening Australia's cyber defences thus far.

As we look towards Horizon 2's main objective to "Expand our reach," we must address a critical gap hindering our national ambition: a severe lack of investment and commercial drive in our domestic cyber security industry and respective ecosystem. While total venture capital funding in Australia reached $4.0 billion in 2024, cyber security is excluded from top-funded sectors such as Fintech and Climate Tech; only 0.7% (AUD $29M) of Australian startup funding reached early-stage cyber security companies. This underinvestment is stark when compared to global innovation hubs. As a key reference, during 2024, Israeli cyber security companies alone raised $3.8 billion, nearly equivalent to Australia's entire startup funding across all sectors. This disparity highlights a market failure and a significant missed opportunity.

From our perspective as a cyber security-focused venture creation fund, a thriving, sovereign innovation ecosystem is the engine that will power all six of Australia's cyber shields. To achieve this, we propose that Horizon 2 introduces a dedicated, cross-cutting Innovation & Commercialisation Chapter. This chapter must contain specific, potent mechanisms to promote private investments and translate our world-class research into globally competitive companies. These mechanisms should be easy to deploy, consume and measure.

Waiting for a later stage to implement these aspects will result in not achieving the full cyber security potential of Australia. It would mean failing to take advantage of great timing globally, where nations are expanding their defence budgets amid geopolitical uncertainties. Australia can gain from building and investing in creating an innovation hub for cyber security, becoming a global powerhouse and increasing Australia’s national sustainability capabilities.

4. Justification for an "Innovation & Commercialisation" Chapter

A dedicated focus on innovation is essential to achieving the 2030 vision and becoming a cyber world leader. It is the mechanism by which Australia can transition from being a consumer of foreign-built cyber defences to a producer of world-class sovereign technology solutions.

- **Addressing Australia's Unique Challenges:** Many of Australia's cyber security challenges are both extreme and unique, from securing vast and remote critical infrastructure to protecting a highly digitised economy spread across a massive geography. A local innovation ecosystem can develop tailored solutions that are often more effective and cost-efficient than off-the-shelf global products. Furthermore, a vibrant domestic industry would drive global tech players to treat the Australian market more seriously, ensuring our specific needs are met. This is in addition to the immense economic benefits of job creation, IP generation and potential export revenues.
- **Innovation Underpins All Six Shields:** A robust innovation ecosystem is not an isolated goal for Shield 5; it is the critical enabler for all six shields.
    - It produces the advanced, automated tools needed for Shield 3 (Threat Sharing and Blocking), moving beyond manual processes to machine-speed defences.
    - It creates secure-by-design products for Shield 2 (Safe Technology), ensuring connected devices and critical software are built with security at their core and not as an afterthought.
    - It develops accessible, scalable and affordable solutions for Shield 1 (Strong Businesses and Citizens), particularly for SMEs who are disproportionately targeted but lack the resources for enterprise-grade tools.
    - It delivers the specialised, resilient technologies required to defend Shield 4 (Protected Critical Infrastructure), from our energy grids to our water supplies.

  Without a thriving innovation engine, our shields will be built with imported technology, limiting our sovereign control and economic benefit.
- **Addressing the "Valley of Death":** Australia employ world-class academic research capabilities and a vibrant startup scene; however, it lacks a persistent framework that connects breakthroughs and commercial success. This "valley of death" is where promising ideas, whether from a university lab or a founder's garage, perish. While the challenge often begins with a lack of early-stage, high-risk capital, it is equally driven by a shortage of experienced commercial and entrepreneurial talent to guide startups. A dedicated chapter can

introduce targeted initiatives to bridge this gap, ensuring that both taxpayer-funded research and local ingenuity translate into sovereign economic and security benefits, rather than being commercialised overseas or failing to launch.

- **Building a Self-Sustaining Ecosystem:** The ultimate goal is to create a self-sustaining ecosystem where success begets success, creating a powerful flywheel effect. This requires more than funding individual projects; it demands building a permanent infrastructure, specialised funds, accelerators and talent pipelines that can systematically produce new ventures over the long term. In mature ecosystems like Israel, successful cyber security exits create a new generation of experienced founders and angel investors who then fund and mentor the next wave of startups. This virtuous cycle is what builds lasting industrial strength. Australia's ecosystem is not yet at this stage and government action is needed to kickstart the flywheel.
- **Global Competitiveness & The Need for Government to Lead:** The global cyber security market is intensely competitive. To nurture robust sovereign capabilities, Australia must create an environment that is as attractive for founders and investors as leading innovation hubs like Israel and the US Crucially, government action is required to catalyse this market. Unlike more mature tech sectors, Australia lacks a deep history of large-scale cyber security startup exits that private investors can rely on for confidence. In nascent, high-risk sectors of national importance, the Australian investment community often looks to the government to act first, to de-risk the landscape and signal a clear national priority. This makes the inclusion of these initiatives in Horizon 2, not a later stage, absolutely critical to building market momentum.

5. Detailed Proposed Initiatives for the Innovation & Commercialisation Chapter

To catalyse private investment and translate Australia's world-class research into globally competitive companies, we propose five synergistic initiatives. These ideas are based on the success of similar programs elsewhere and have been adjusted to what UBIQ has analysed as the core needs to build a thriving Australian cyber security startup ecosystem that will support and lead the national strategy. Each has been designed to be actionable using existing Australian Government mechanisms and can be deployed individually, in combination, or as part of a broader program, though there is significant added value in their synergy and ensuring they can be deployed rapidly without new legislation or bureaucracy.

Initiative 1: Cyber Security Venture Capital Co-Investment Fund

- What it is: A government co-investment fund, structurally identical to the successful Biomedical Translation Fund (BTF), to act as a cornerstone investor in private, cyber security-focused venture capital (VC) funds. This is the bold, large-scale option for maximum impact, designed to create several well-capitalised, specialised funds capable of supporting companies from seed to scale. This initiative directly addresses the critical shortage of early-stage private risk capital at a systemic level.
- How it Works:
    - Mechanism: The government would establish a "cyber security Translation Fund (CTF)" as a dedicated investment vehicle. The CTF will operate on a co-investment basis, committing capital as a Limited Partner (LP) into two to three specialised, private-sector cyber security VC funds selected through a competitive tender.
    - Management: The fund would be administered by the Department of Industry, Science and Resources (DISR) and AusIndustry, leveraging their expertise from managing the BTF. The selected private fund managers would have sole responsibility for all investment decisions, ensuring commercial discipline and leveraging their specialist expertise. This "Government as Catalyst, Private Sector as Executor" model mitigates risk and leverages commercial acumen.
    - Funding Model: The government would make a cornerstone investment of $100 million to be at least matched dollar-for-dollar by private capital (e.g., from superannuation funds, institutional investors). This creates a total investment pool of $200+ million dedicated to the sector, achieving the scale required to make a national impact.
- Successful Implementation Example: The Biomedical Translation Fund (BTF) is a

proven Australian success story. This existing, proven framework can be replicated for cyber security, ensuring rapid and efficient deployment.

- Indicative Budget: A balance sheet investment of $100 million in cornerstone capital. This is not a grant expenditure, and the model is designed to provide a financial return to the Commonwealth over the fund's 10-year life.

Initiative 2: Targeted VC Co-Investment Programme

- What it is: An agile and highly-leveraged alternative to the large-scale fund. This programme would directly co-invest in specialised cybersecurity VC funds to amplify their ability to deploy capital into the ecosystem.
- How it Works: The government, via a tender process managed by AusIndustry, would select and invest $8 million into each of up to three specialised cybersecurity VCs.
    - Condition: A key condition would be that the selected VCs must commit to raising a minimum of $30 million AUD in total private capital, ensuring a significant leverage of government funds.
    - Structure: These funds can be subsidiaries of existing VCs but must be established as separate legal vehicles dedicated only to cybersecurity to ensure focus.
    - Measurement: Success would be measured by detailed annual reports, government participation on the fund's board (as an observer or limited partner), and a financial return to the government after a 10-year period. Proceeds from the investment will be reinvested in future cybersecurity innovation funds, either through the same funds or new tenders, creating a self-sustaining model.
- Indicative Budget:
    - Balance Sheet Investment: $24 million ($8M x 3 funds).
    - Programme Administration (via AusIndustry): $2.4 million
    - Total Indicative Budget: $26.4 million

Initiative 3: Direct Investment & Investor Incentives

- What it is: A more granular, programmatic approach to de-risk and attract private capital, composed of two distinct streams that can be implemented together or separately. This initiative can also serve as a more agile alternative if the large-scale fund in Initiative 1 is deemed too significant.

- How it Works:

    1. Stream A: Enhanced cyber security ESVCLP Incentive: A time-limited, five-year program to incentivise investment *into funds*. This uses policy and

regulation to create a "Cyber Focus" designation within the ESVCLP framework. For investors (Limited Partners) in a designated "cyber security ESVCLP," the government, through AusIndustry, would provide a direct, non-taxable rebate of 15% on their contributions, which complements the existing 10% tax offset to deliver a powerful 25% effective incentive. This would be paired with a fast-tracked registration process for qualifying funds.

2. Stream B: Early-Stage Co-Investment Grant: A program to incentivise investment *directly into companies*. For every dollar of eligible private capital invested in an early-stage Australian cyber security company, the government will provide an additional 15 cents as a non-dilutive grant to the company. This grant would be capped at $500,000 per company and the overall program would have an annual budget of $10 million. The process would be managed by AusIndustry with a simple, programmatic approval mechanism to ensure speed and efficiency.

- Successful Implementation Example: The ESVCLP program is a proven framework for Stream A. For Stream B, the R&D Tax Incentive's cash refund component provides a strong precedent for the government making direct, non-dilutive cash contributions to companies to incentivise specific activities.
- Indicative Budget: A combination of direct expenditure dependent on uptake for Stream A, and a capped budget of $50 million over 5 years for Stream B ($10M/year).

Initiative 4: National cyber security Accelerator Program

- What it is: A dedicated grant program to attract and support world-class, specialised cyber security accelerators and venture builders. This initiative builds the "factory floor" of the innovation ecosystem, creating the sustainable, private-sector infrastructure needed to systematically produce and fund new companies. A world-class accelerator provides intensive mentorship, access to global customer and investor networks, and deep technical expertise that is otherwise unavailable to early-stage founders.
- How it Works: A multi-year, contestable grant program, administered by AusIndustry, to support the operational costs of up to two national accelerator programs. A tender process would select the programs, and providing multi-year funding ensures the long-term certainty needed to attract top-tier global operators and build sustainable infrastructure. The budget is calculated to provide substantial operational funding of $2 million per year for 5 years to each of the two selected programs ($2M/year x 2 programs x 5 years = $20M), plus an allocation for administration.
- Successful Implementation Example: LaunchVic in Victoria has demonstrated how government support for accelerators can build a vibrant, specialised startup

ecosystem. Applying this proven playbook nationally is a low-bureaucracy, high-impact approach.

- Indicative Budget (over 5 years):
    - program Grants: $20 million
    - program Administration (via AusIndustry): $2 million
    - Total Indicative Budget: $22 million

Initiative 5: Venture Fund Establishment Grants

- What it is: A targeted grant program to lower the barriers to entry for new, private-sector, cyber security-focused VC funds establishing in Australia. The goal is to increase the number of specialised fund managers who can provide not just capital, but also deep domain expertise and global networks, which is a critical missing piece in the current Australian ecosystem.
- How it Works: A contestable grant round, administered through AusIndustry, offering grants of up to $500,000 to cover the high initial operational and regulatory costs of establishing a new venture fund (e.g., legal, compliance, initial salaries). This encourages the formation of the specialised investment expertise our ecosystem needs. The budget is designed to support the establishment of up to three new funds, with each receiving a grant of $500,000 ($500,000 x 3 funds = $1.5M), plus a provision for administration.
- Successful Implementation Example: This model was also used effectively by LaunchVic to attract new fund managers to Victoria, proving its ability to catalyse the formation of private capital vehicles.
- Indicative Budget (over 5 years):
    - program Grants: $1.5 million
    - program Administration (via AusIndustry): $0.25 million
    - Total Indicative Budget: $1.75 million

Initiative 6: Prioritising R&D Commercialisation Pathways

- What it is: This initiative focuses on prioritising cyber security within existing, highly effective government R&D commercialisation structures, ensuring taxpayer-funded research translates into sovereign capability without creating new administrative bodies. It directly tackles the "valley of death" by focusing existing resources and strengthening academia-industry-government collaboration, providing a direct route for cutting-edge research to become Australian-owned commercial products.

- How it Works (Implementation Details):
    - "CyberGov Labs" via the Business Research and Innovation Initiative (BRII): Instead of a new program, this establishes a dedicated and recurring "National Cyber Security Challenge" stream within DISR's existing BRII program. Government agencies (e.g., Home Affairs, ASD, Defence) would define high-priority, unclassified challenges, and BRII would provide grants to SMEs to develop innovative solutions.
    - cyber security Translation Grant Top-Up via the ARC: To bridge the gap between academic research and commercial application, this enhances existing Australian Research Council (ARC) grants (e.g., Linkage Program) with a supplementary "Cyber Commercialisation Bridge" grant. Research teams with projects demonstrating high potential for cyber security commercialisation could apply for a top-up grant of $50,000-$100,000, conditional on securing a formal partnership with an industry or venture capital entity.
- Successful Implementation Example: The BRII program has already run a successful Cyber Security Challenge, providing a direct precedent. Formalising this into a recurring stream creates a predictable and efficient pathway for government agencies to solve real-world problems.
- Indicative Budget (over 4 years): An additional allocation of $5-10 million to run the prioritised streams within BRII and the ARC.

6. Measuring Success (5 and 10-Year Horizons)

To ensure accountability, we propose the following success metrics be evaluated over 5 and 10-year periods.

Metric	5-Year Target (Establishment & Growth)	10-Year Target (Maturity & Global Impact)	Initiative Supported
Capital Mobilised	Attract at least $3 of private capital for every $1 of government investment/expenditure across all co-investment and incentive programs.	Achieve a 6:1 private-to-government capital leverage ratio. Supported companies are successfully raising significant later-stage international capital.	1, 2, 3, 5
New Venture Creation	At least 15 new, high-potential cyber security startups funded and actively scaling through the supported funds and programs.	The ecosystem is sustainably producing 10+ new funded ventures annually. At least two supported companies have achieved 'unicorn' status ($1B+ valuation).	1, 2, 3, 4
Job Creation	Creation of over 300 high-skilled cyber security, engineering, and commercial jobs within the companies supported by the initiatives.	Creation of over 1,500 high-skilled jobs. A measurable increase in talent retention, with experienced professionals choosing to build careers in Australia.	All Initiatives
R&D Commercialisation	At least 15 significant research projects or patents commercialised from Australian universities and CRCs through the prioritised R&D pathways.	A self-sustaining pipeline exists between research institutions and industry, with Australian universities recognised globally as top-tier sources of cyber innovation.	6
Sovereign Capability	Significant Joint projects	Australian sovereign	All Initiatives

Uplift	or Australian developed solutions procured and deployed by Australian government agencies and critical infrastructure operators. Measured by # of solutions deployed per company and % of budget invested in Australian made products.	solutions are actively protecting a growing portion of our critical infrastructure, measurably reducing reliance on foreign technology. Measured by # of solutions deployed per company and % of budget invested in Australian made products.	
Global Competitiveness	At least 5 supported companies have successfully expanded into international markets and are generating export revenue.	Australia is recognised as a top-5 global hub for cyber security innovation. Multiple supported companies are category leaders in international markets.	1, 2, 3, 4

7. Summary and Conclusion

To "Expand our reach" in Horizon 2, Australia must move beyond foundational policies and actively build the engine of innovation. The initiatives proposed are practical and synergistic. To ensure immediate impact, we recommend a high-priority package to build the foundational infrastructure and stimulate capital. This would include the National Cybersecurity Accelerator Programme and Venture Fund Establishment Grants as essential ecosystem-building blocks, paired with the agile and highly-leveraged Targeted VC Co-Investment Programme as the core capital stimulus.

This recommended package represents a combined investment of approximately $50 million and provides the most efficient and impactful start to building a sovereign innovation ecosystem. The Prioritising R&D Commercialisation Pathways initiative can be highly effective by leveraging existing departmental funds. With this targeted commitment, the government can send a powerful signal to the market. This is critical, as the Australian investment community looks to the government to initiate and lead in areas of national importance. Government action is the catalyst required to de-risk the sector for private capital and kickstart the flywheel of a self-sustaining, world-class cybersecurity ecosystem.

Proposed Initiative	Indicative Budget	How it Supports the Six Shields
Cyber Security Venture Capital Co-Investment Fund	$100M (Balance Sheet)	**Shield 5:** Fuels industry growth. **Shield 1:** Creates more tools for SMEs. **Shield 2:** Funds secure-by-design tech.
Targeted VC Co-Investment Programme	$26.4M (Balance Sheet & Admin)	**Shield 5:** Directly fuels multiple specialised funds. **Shield 1 & 2:** Increases capital available for new sovereign solutions.
Direct Investment & Investor Incentives	$50M+ (Direct Expenditure)	**Shield 5:** Aggressively channels private capital to cyber funds & startups. **Shield 1 & 2:** Increases capital for new solutions.
National cyber security Accelerator program	$22M (Grants)	**Shield 5:** Builds the "factory floor" for new companies and develops talent. **Shield 4:** Can target critical infrastructure tech.

Venture Fund Establishment Grants	$1.75M (Grants)	**Shield 5:** Increases the number of specialised cyber investors in Australia, building ecosystem maturity.
Prioritising R&D Commercialisation Pathways	$5-10M (Grants)	**Shield 5:** Directly translates research into sovereign capability. **Shield 2:** Commercialises cutting-edge safe technology.

By adopting at least some of these measures as suggested above, the Australian Government can create the conditions for a truly world-leading cyber security ecosystem, ensuring our nation is not only well-defended but is also at the forefront of creating the technologies that will secure our digital future.

We look forward to collaborating further as you develop Horizon 2.