cydarm

Department of Home Affairs
Submitted electronically via Department of Home Affairs Submission Form

29 August 2025

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

Cydarm Technologies Pty Ltd (Cydarm) welcomes the opportunity to provide input on the questions raised in Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy, released in July 2025.

Cydarm is an Australian owned and operated software company, founded in 2017, that makes Cybersecurity Incident Response Management (CIRM) software for customers in Australia and abroad. The Cydarm CIRM platform is used by customers in Government and Critical Infrastructure to make cybersecurity operations better and faster, enabling organisations to perform more effectively and efficiently across the entire incident response lifecycle.

Cydarm's position as a cybersecurity vendor funded by Australian venture capital (ESVCLP), along with the experience of our founders, and our network of peer organisations also developing sovereign capability ("startups") gives us a perspective on how public policy can affect the cybersecurity through the lens of collective defence as well as the lens of sovereign technology.

Q29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

At its foundation, intelligence sharing is about providing timely indicators of compromise and attack techniques so that organisations can defend themselves and each other. Shared indicators enable collective defence: when one organisation sees a threat, others can prepare for it.

The ACSC already provides this capability through CTIS, with structured threat intelligence in STIX (Structured Threat Information eXchange) format. The other threat intelligence distribution mechanism is via PDF advisories containing long tables of indicators. While these PDFs are valuable for awareness, they are not operationally efficient: teams must manually extract and translate data into formats suitable for tooling, which slows response.

A practical improvement would be to publish downloadable STIX bundles alongside existing PDF advisories. Unlike the broad CTIS feed, these would be targeted to the specific threat described in the advisory, providing ready-to-ingest intelligence that directly supports defensive actions. CISA in the US has been doing this for many years, demonstrating that targeted, structured bundles are far more actionable than long PDF tables alone.

The next stage is to extend beyond indicators into actionable defensive tradecraft. Playbooks, structured using open standards (eg. CACAO - Collaborative Automated Course of Action Operations), allow advisories to include recommended actions such as blocking malicious domains, updating detection rules, or notifying affected customers. Playbooks provide common structure, clarify roles and responsibilities, and scale across organisational maturity levels - from large SOCs to smaller IT providers.

By first strengthening indicator sharing through targeted STIX bundles, and then extending into CACAO playbooks, Australia can turn threat intelligence from static information into operational, repeatable, and collaborative defence capability, strengthening cyber security and scam prevention at scale.

Q44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

Australia is a nation girt by sea. As such, we rely on undersea cables for our communications with the rest of the world. Our unique geography and current geopolitics means that we need to increase self-reliance. We cannot depend entirely on foreign organisations to provide us with the technology that is the backbone of modern society. Even when our data is located in sovereign data centres in Australia, if we are over-reliant on foreign technology specialists to provide remote troubleshooting, patches, and upgrades to our systems, we are vulnerable. As such, it is imperative that we increase sovereign capability.

To identify and prioritise sovereign capabilities, the focus should be on demand and adoption, not just supply. The strongest signal of a capability worth scaling is when the government or industry is willing to pay for it. Customer revenue is a more reliable validator than government grants.

Government's role should be to act as a lead customer where sovereign control is essential, creating predictable demand that allows sovereign companies to scale. That creates stronger incentives than grant programs, which too often reward grant-writing rather than product delivery, wasting the time and resources of sovereign companies, and distorting the demand signal from customer revenue.

For growth capital, the priority should be sovereign venture capital investing in sovereign product companies. Government is not well placed to pick winners, but it can create the conditions for private capital to do so - for example, co-investment structures and policy settings that favour domestic funds deploying into domestic capability. Israel's YOZMA program is a proven model: rather than governments selecting companies, they seeded local venture capital funds with private partners, which went on to build one of the world's strongest innovation ecosystems.

It’s also critical to ensure that sovereign technology is actually built here. Local development stimulates STEM participation, reverses brain drain, and ensures expertise is domiciled in Australia rather than lost offshore. Without these safeguards, we risk “sovereign washing” - foreign tech firms dressing up local sales, token R&D, or “investment” as sovereign capability, when in practice it consolidates their footprint and extracts value offshore, to the detriment of sovereign vendors and our economy. That approach builds dependency, not resilience.

In short, the path forward is:

- Define sovereign needs in terms of outcomes, not technologies.
- Signal priorities through procurement, not grants.
- Back sovereign venture capital to scale sovereign product companies, following proven models like YOZMA.
- Require genuine local build and expertise, to grow the STEM workforce, retain talent, and ensure sovereign capability is more than a branding exercise.

That combination ensures capabilities are grounded in real demand, disciplined by market signals, scaled with aligned private capital, and genuinely sovereign.