SHM Advisory
CYBER DONE BETTER

SHM Advisory Submission

2023-2030 Australian Cyber Security Strategy - Horizon 2 Consultation

Submitted by: [redacted], SHM Advisory
Date: August 2025
Contact: CSSH2@homeaffairs.gov.au

Introduction

About SHM Advisory SHM Advisory provides strategic cybersecurity consulting services to organisations across Australia, helping them navigate complex security challenges and build resilient cyber capabilities. Our expertise spans government, enterprise, and emerging technology sectors.

Submission Author: Shane Moffitt This submission is prepared by Shane Moffitt, Principal of SHM Advisory, bringing extensive cybersecurity leadership experience across government and enterprise sectors:

- **Former Deputy Chief Information Security Officer, Victorian Government** - Led state-level cybersecurity strategy implementation, including the successful deployment of the Cyber State Purchase Contract that delivered transformational procurement efficiencies and cost savings
- **Former Oceanian Information Security Lead, Ernst & Young** - Provided regional cybersecurity consulting across enterprise clients, developing deep expertise in security frameworks, risk management, and technology implementation at scale
- **Principal, SHM Advisory** - Currently advising organisations on cybersecurity strategy, governance, and practical implementation challenges

Understanding the Real Challenge After decades of working in government and enterprise cybersecurity, a fundamental truth has become clear: **most cybersecurity problems have known and proven solutions**. The technologies exist, the frameworks are established, and the methodologies are well-documented. Anti-malware, vulnerability scanning, application control, multi-factor authentication, and security monitoring aren't emerging technologies that need research and development.

The real challenge isn't deciding what to do, but how to put proven solutions into action in a timely manner.

Government cybersecurity initiatives often get stuck in long procurement processes, repeated assessments, fragmented vendor relationships, and inconsistent ways of implementing solutions. While agencies spend months or years assessing solutions that enterprises roll out in weeks, malicious actors keep exploiting the gaps.

Our Perspective on Horizon 2 As Australia moves from Horizon 1's foundational efforts to Horizon 2's ambitious aim of expanding cyber maturity across the entire economy, the emphasis must shift to **implementation pace and consistency**. Success will be judged not by how advanced our strategies are, but by how swiftly and effectively we can roll out proven cybersecurity solutions across all levels of government.

The insights shared in this submission are based on practical experience implementing cybersecurity initiatives within government, consulting with major enterprises across Oceania, and current market observations of what accelerates and impedes cybersecurity implementation.

Key Recommendations Overview

This submission focuses on two strategic recommendations that can significantly accelerate Australia's ability to implement proven cybersecurity solutions during Horizon 2:

1. **Establish Standardised IT Procurement Framework** - Leveraging proven success from Victorian Government's Cyber State Purchase Contract
2. **Establish Standardised Security Assurance Programme** - Building on the DTA Hosting Certification Framework model

Both recommendations address core implementation barriers while enhancing sovereign capability, cost efficiency, and security outcomes across all levels of Australian government.

Recommendation 1: Establish a Standardised IT Procurement Framework

The Enterprise Standard: Global Best Practice: Every major enterprise globally, from multinational corporations to leading technology companies, standardises its core technology stack. This isn't just a preference; it's a fundamental requirement for operational efficiency, security consistency, and cost management at scale. The same principle that drives ASX 200 companies to standardise their cybersecurity tools should guide government procurement.

Complexity Reduction: A Strategic Imperative: Technology stack complexity is the enemy of both security and efficiency. When government agencies operate disparate security solutions across departments, it creates:

- Inconsistent security postures and gaps
- Increased attack surfaces
- Fragmented visibility and incident response capabilities
- Exponential management overhead

Victorian Government: Proven Results: During my time as Deputy Chief Information Security Officer, I saw firsthand the transformation brought about by the Cyber State Purchase Contract (SPC). The results were significant:

- **Procurement Timeline**: Reduced from up to 9 months to one week
- **Process Efficiency**: Eliminated repetitive vendor evaluations and negotiations
- **Cost Savings**: Expected $100 million in direct savings over the 5-year SPC lifecycle

Federal Government Opportunity: Extrapolating the Victorians' $100 million savings across the federal government's significantly larger scale suggests potential savings of **$500-800 million** over a similar timeframe, considering the federal government's broader scope and higher technology spending.

Maintaining Competitive Tension: The framework should establish a supplier pool of about three vendors per technology category. This maintains healthy competitive tension while avoiding the inefficiencies of unlimited vendor proliferation. Three suppliers provide:

- Sufficient competition to drive innovation and pricing
- Manageable vendor relationships for government
- Backup options for service continuity
- Competitive benchmarking opportunities

Flexible Implementation: Non-Mandatory Framework: The standardised procurement framework should not be mandatory, permitting agencies to deviate when justified by:

- **Special operational requirements** that standard solutions cannot address
- **Breakthrough technology adoption** that offers significant security or capability advantages
- **Mission-critical needs** requiring specialised or emerging solutions
- **Urgent threat response** requiring immediate technology deployment

This flexibility ensures the framework speeds up standard procurement while maintaining agencies' ability to innovate and address specific challenges.

Driving Sovereign Capability and Data Sovereignty: A standardised procurement framework creates appealing commercial conditions for suppliers to invest in Australian-based operations. Large, predictable government contracts encourage vendors to:

- Establish Australian data centres and hosting infrastructure
- Hire and train local cybersecurity talent
- Develop sovereign capability within Australia
- Meet data sovereignty requirements through local operations
- Contribute to Australia's cyber security ecosystem growth

Centralised Expert Vetting: Rather than duplicating security assessments across thousands of agencies, a centralised framework enables:

- **Expert-level security evaluation** by specialised government cybersecurity professionals
- **A comprehensive capability assessment** to be conducted once and applied nationally
- **Ongoing monitoring** of vendor security levels and compliance

- **Standardised security requirements** that vendors can build towards
- **Reduced the burden** on individual agencies lacking deep cybersecurity expertise

Operational Efficiency Multipliers: Standardisation delivers compounding benefits:

- **Technology Compatibility**: Seamless integration and data sharing between agencies
- **Reduced Training Costs**: Support staff expertise becomes transferable across agencies
- **Streamlined Management**: Single vendor relationships and unified support models
- **Enhanced Security**: Consistent patch management, configuration standards, and threat intelligence sharing

This approach shifts government cybersecurity from a fragmented, reactive model to a strategic, proactive capability that enhances security outcomes and economic benefits while keeping the agility to adopt innovative solutions when necessary.

Recommendation 2: Establish a Standardised Security Assurance Programme

Learning from Proven Success: The DTA Hosting Certification Framework Australia already has a successful model for standardised security assurance. The Digital Transformation Agency's Hosting Certification Framework "has significant benefits to government and industry and operationalises the principles outlined in the Whole-of-Government Hosting Strategy". This framework shows how centralised assessment can be practical while "Government entities continue to have the autonomy to select the best hosting arrangements for their requirements"

The Current Challenge: Fragmented Supplier Security Assessment: Across Australian federal, state, and local governments, agencies independently carry out security assessments of the same vendors, leading to inefficiency and inconsistency. A provider may face numerous separate security reviews from different government bodies, each with different standards, requirements, and assessment methods.

Expanding the Hosting Framework Model: The success of the DTA framework should extend beyond hosting to encompass the entire supply chain of providers. The Framework "provides guidance to Australian Government departments and agencies enabling them to identify and source hosting services that meet enhanced privacy, sovereignty and security requirements" - this same approach should apply. to all critical technology suppliers.

Drawing from Enterprise and Government Experience: From my experience at Ernst & Young, leading Oceanian information security initiatives, multinational enterprises maintain centralised supplier security assessment programmes that scale across regions and business units. Similarly, during my time as Deputy Chief Information Security Officer for the Victorian Government, the lack of standardised supplier assurance caused operational friction and security gaps

A National Security Assurance Framework: Australia needs a standardised security assurance programme that operates across all three levels of government, federal, state, and local. This programme would expand the proven DTA model to include:

1. **Centralised Assessment and Accreditation:** While the DTA has demonstrated success with the Hosting Certification Framework, it would not have the capacity to vet all suppliers across the expanded scope required centrally. This function would need to be outsourced through a programme similar to the Information Security Registered Assessors Program (IRAP), where accredited private sector assessors conduct standardised evaluations under government oversight.
    - **Single security evaluation process** conducted by IRAP-style accredited assessors rather than individual agency procurement teams
    - **Standardised security requirements** aligned with the Australian Government Information Security Manual (ISM) and international frameworks
    - **Tiered accreditation levels** based on data classification and risk profiles
    - **Continuous monitoring** of supplier security postures rather than point-in-time assessments
    - **Quality assurance oversight** by the government to ensure consistency across accredited assessors
2. **Operational Benefits**
    - **Eliminate Duplicated Efforts**: Stop the current practice where suppliers undergo multiple identical assessments across agencies
    - **Consistent Standards**: Ensure consistent security expectations across all government levels
    - **Expert Assessment**: Utilise specialist cybersecurity expertise instead of general procurement skills.
    - **Faster Onboarding**: Pre-assessed suppliers can engage with new agencies immediately
3. **Supplier Chain Risk Management** Drawing from enterprise risk management practices, the programme should address:
    - **Third-party risk assessment,** including subcontractors and dependencies
    - **Supply chain transparency** requirements for critical technology providers
    - **Ongoing compliance monitoring** rather than one-time assessments
    - **Incident response coordination** when supplier security events occur
4. **Economic and Security Multipliers**
    - **Cost Reduction**: Suppliers bypass multiple assessment processes, lowering their costs and government pricing
    - **Security Enhancement**: Consistent, expert-led reviews enhance overall security results

- **Market Efficiency**: Clear, standardised requirements assist suppliers in making proper security investments.
- **Innovation Enablement**: Streamlined processes enable quicker adoption of new security technologies

Implementation Considerations

- **Mutual Recognition**: Assessments conducted at the federal level are automatically recognised by state and local governments
- **Risk-Based Approach**: Assessment depth scaled according to data sensitivity and operational importance
- **Regular Review Cycles**: Regular review aligned with evolving threat landscape
- **Appeals Process**: Mechanism for suppliers to address assessment outcomes

This standardised approach turns supplier engagement from a fragmented, inconsistent process into a strategic capability that improves both security outcomes and operational efficiency across all levels of Australian government, building on the proven success of the DTA Hosting Certification Framework.

Conclusion

Horizon 2's success in improving cyber maturity across Australia's economy fundamentally relies on our ability to quickly and reliably implement proven solutions. The two recommendations in this submission—standardised IT procurement and security assurance frameworks—directly tackle the barriers to implementation that currently prevent the government from deploying cybersecurity solutions at the necessary speed and scale. Both recommendations build on established Australian successes: the Victorian Government's Cyber State Purchase Contract and the DTA's Hosting Certification Framework. They offer clear paths to reduce costs, improve security outcomes, strengthen sovereign capability, and accelerate the deployment of proven cybersecurity solutions.

The opportunity ahead is significant. We can reshape how Australian governments acquire, assess, and use cybersecurity capabilities, creating a model that positions Australia as a global leader in efficient and effective cybersecurity practices.

SHM Advisory is ready to assist with developing and implementing these frameworks, drawing on our combined government and enterprise experience to help Australia achieve its Horizon 2 goals.

For further discussion of these recommendations, please contact:
[redacted]
SHM Advisory
[redacted]