NIIN

National Industry Innovation Network

Securing the Nation

Accelerating Government Cyber Security in an Age of Digital Disruption

Frank den Hartog | UNIVERSITY OF CANBERRA
Ellie Liu | UNIVERSITY OF CANBERRA
Daniella Gullotta | UNIVERSITY OF CANBERRA
Sarah Sloan | CISCO

Strategic Partnerships

Skills + Talent Development

Innovation CentralNetwork

Specialised Centres

Cyber + Health Alliances

Research Chair Program

Industry AlumniProgram

Executive Summary

Australia is facing accelerating cyber risk as threats grow more sophisticated, technologies evolve rapidly, and uplift across government entities remains uneven. Recent audits and posture assessments reveal that the implementation of mandatory frameworks, including the Protective Security Policy Framework (PSPF), and the Essential Eight, continues to lag, leaving critical systems exposed at a time when cyber, Artificial Intelligence (AI)-enabled and quantum threats are intensifying. At the same time, uplift is not occurring at the speed or scale required by the 2023–2030 Cyber Security Strategy, widening the gap between policy ambition and operational reality.

This gap is reinforced by systemic barriers that limit governments' ability to strengthen and sustain their security posture. Funding and approval processes remain geared toward capital intensive, point in time initiatives, which are misaligned with the continuous, operational nature of cyber security. Annual audit cycles reinforce a compliance driven culture, reducing the focus on real-time visibility of risk. Legacy Information and Communication Technology (ICT) environments, which represents a significant form of "technical debt" compounds these challenges by constraining uplift efforts, while ongoing workforce shortages limit agencies' capacity to operationalise contemporary capabilities.

Meanwhile, new classes of critical systems, Systems of Government Significance (SoGS), have been defined and are in the early stages of uplift. The lack of standardised, risk-based prioritisation and limited visibility of their technical state further slows progress, despite SoGS representing the nation's most consequential digital functions. Early prioritisation and clearer engagement with technology providers would accelerate uplift and ensure these high-impact systems receive the protection their national importance demands.

Emerging technologies add further urgency. The adoption of AI across the government is increasing but remains uneven, with governance, guardrails and secure by design practices not keeping pace with agency demand. Meanwhile, growing awareness of Post-Quantum Cryptography (PQC) risk has not yet translated into practical readiness, with many entities still struggling to plan, prioritise and sequence migration to PQC at the pace required.

For government to close the widening gap between policy objectives and operational resilience, a more coordinated, centrally supported and risk-led approach is essential. The following recommended actions will help strengthen national readiness and accelerate uplift.

RECOMMENDATIONS

1. **Close the policy-to-practice gap**: Accelerate uplift of critical systems through practical implementation pathways for PSPF including AI and PQC readiness, supported by centralised funding and continuous reporting.
2. **Augment point-in-time audits with continuous cyber assurance — particularly for critical systems**: Organisations should complement point-in-time audits with real-time visibility and continuous assurance to improve security posture visibility and responsiveness to emerging threats.
3. **Make the uplifting of SoGS a strategic priority**: Direct early, risk-based and coordinated investment toward systems whose failure would have the most substantial public, economic or national security impact.
4. **Strengthen the messaging surrounding the requirements of SoGS**: Build structured engagement with technology providers to ensure clear understanding and delivery of security expectations for SoGS.
5. **Review New Policy Proposals (NPP) and budget processes to support preventative, risk-based cyber investment**: Funding and approval mechanisms should be adapted and aligned to prioritise investments based on assessed risk and system criticality, rather than favouring incident-driven remediation, or visibly failing systems.
6. **Introduce greater flexibility for Operational Expenditure (OpEx)-based and multiyear cyber investments**: Governments should review the current investment frameworks to ensure they are fit for purpose in supporting modern cyber security resilience and operational efficiency. Funding models should better accommodate the operational nature of cyber security, including cloud, Software-as-a-Service (SaaS), monitoring, and detection capabilities, to reduce reliance on Capital Expenditure (CapEx)-centric decision making.
7. **Drive cyber defence through a risk management lens**: Prioritise controls and funding based on organisational context and value, threat exposure, assets criticality, impact and Root Cause Analysis (RCA), and let those priorities determine the pathway toward compliance obligations.
8. **Review the Essential Eight for its suitability for government systems**: Review the Essential Eight to assess its suitability for modern day cyber security uplift across cloud, SaaS, identity-centric environments, and emerging threats, including AI-enabled attacks. Consider if additional guidance, flexibility, or targeted investment may be required to support consistent uplift across government.

9. **Accelerate coordinated action on legacy and End-of-Life (EoL) ICT, particularly across SoGS**: Agencies should be required to maintain live technology asset registers identifying legacy and EoL systems, supported by whole-of-government prioritisation and targeted replacement or isolation strategies. Capture the role of EoL technology in Incident reporting to improve transparency and inform risk-based responses.
10. **Introduce targeted funding mechanisms for high-risk legacy systems (EoL) replacement and strengthen legacy retirement levers**: Government should consider dedicated "rip and replace" or technical debt reduction funding for the highest risk legacy systems that materially inhibit cyber uplift and resilience. Use procurement, regulatory and targeted investment mechanisms to accelerate retirement of high-risk legacy systems.
11. **Harness AI to strengthen cyber defence**: Implement secure by design AI and leverage defensive AI capabilities to enhance system monitoring, detection and response.
12. **Treat quantum computing as a systemic risk and make the transition to PQC a long-term strategy**: Position PQC uplift as a whole-of-government resilience priority with clear migration pathways, especially for complex and interconnected systems. Plan PQC adoption as a phased, multiyear transformation of government cryptographic foundations, rather than a discrete technical update.
13. **Reduce jurisdictional variability**: Incentivise consistent security requirements across federal, state and territory entities to reduce fragmented uplift.
14. **Expand cyber incident reporting requirements to Australian Signals Directorate (ASD) for all government entities**: Incident reporting obligations should be extended beyond Non-Corporate Commonwealth Entities (NCCEs) to include all Commonwealth entities, improving national situational awareness and coordinated response capability. Work with states and territories to raise awareness of and incentivise reporting.
15. **Address the cyber skills gap to create, attract, and retain a cyber workforce**: Invest in targeted workforce uplift, leadership capability development and retention strategies to sustain secure digital operations.

Australia's window to uplift cyber resilience is narrowing rapidly, driven foremost by an increasingly volatile geopolitical climate that is compressing the time organisations have to act. This urgency is compounded by the approaching transition to Horizon Two of the Strategy. By shifting from compliance driven activity to system-wide, continuous uplift, the government can strengthen the resilience of critical systems and better position itself to withstand the accelerating threats shaping the digital environment.

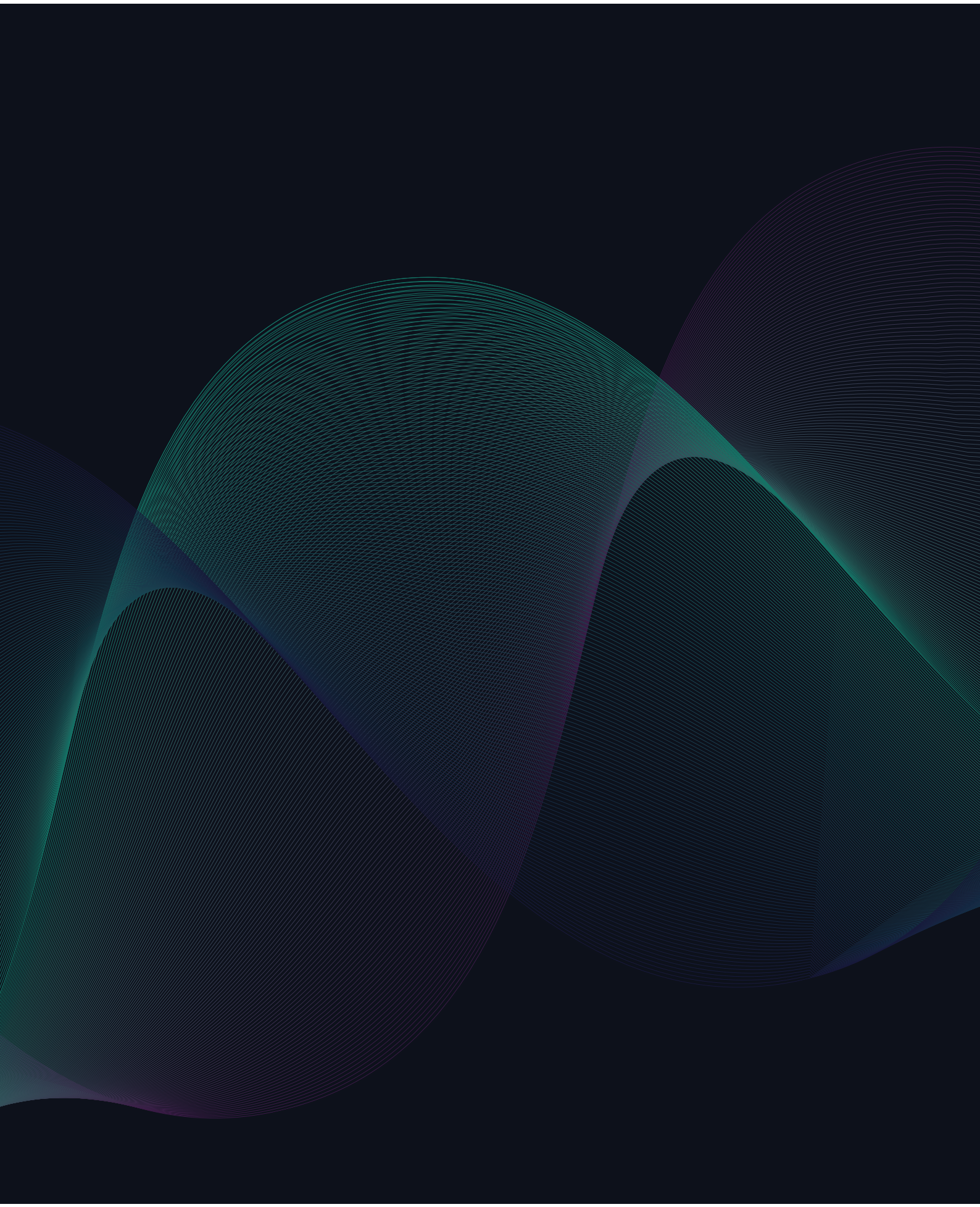
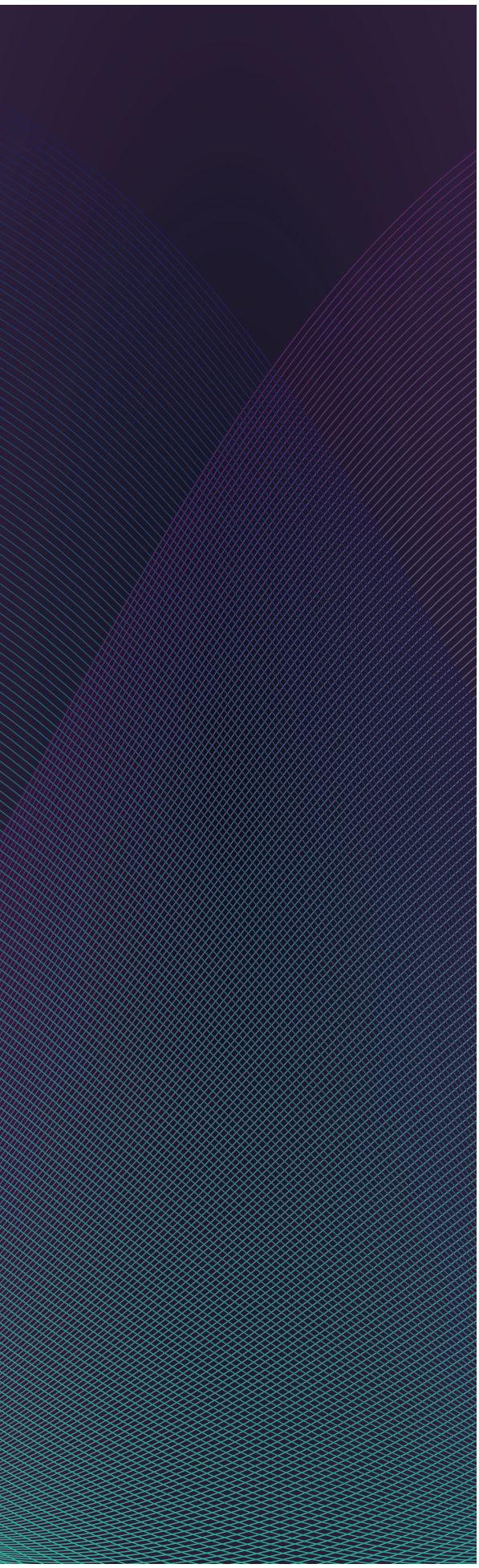


Table of Contents



ABBREVIATIONS

ACSC	Australian Cyber Security Centre
ACT	Australian Capital Territory
AI	Artificial Intelligence
ANAO	Australian National Audit Office
APSC	Australian Public Service Commission
ASD	Australian Signals Directorate
CapEx	Capital Expenditure
CBOM	Cryptographic Bill of Materials
CC	Commonwealth Company
CCE	Corporate Commonwealth Entity
CHIP	Cyber Hygiene Improvement Program
CISC	Critical Infrastructure Security Centre
CPS	Core Practice Standards
CRQC	Cryptographically Relevant Quantum Computer
CSP	Cyber Security Policy
CTIS	Cyber Threat Intelligence Sharing
DHA	Department of Home Affairs
DTA	Digital Transformation Agency
EoL	End-of-Life
EoS	End of Support
EoSS	End of Security Support
HNDL	Harvest Now, Decrypt Later
ICT	Information and Communications Technology
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
JACSD	Justice and Community Safety Directorate
MFA	Multi-Factor Authentication
NCCE	Non Corporate Commonwealth Entity
NIST	National Institute of Standards and Technology
NPP	New Policy Proposal
NSW	New South Wales
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
OpEx	Operational Expenditure
PGPA	Public Governance, Performance and Accountability Act
PQC	Post Quantum Cryptography
PSF	Protective Security Framework
PSPF	Protective Security Policy Framework
RCA	Root Cause Analysis
RMF	Risk Management Framework
SaaS	Software-as-a-Service
SOCI	Security of Critical Infrastructure Act
SoGS	Systems of Government Significance
SoNS	Systems of National Significance
U.S.	United States
UK	United Kingdom

1. The need to accelerate government cyber security in an age of disruption

Australia is among the top ten most targeted countries for cyberattacks globally (Microsoft, 2025). As the nation enters Horizon Two of the 2023-2030 Australian Cyber Security Strategy (Department of Home Affairs [DHA], 2023), from here called "the Strategy", this white paper assesses Australia's preparedness to withstand evolving digital threats and strengthen resilience with a focus on government information systems.

Australia's government systems face mounting pressure to deliver secure, resilient digital services in an increasingly hostile cyber environment. The Strategy sets a bold national vision, supported by policy frameworks such as the the Protective Security Policy Framework (PSPF) (Australian Government, 2025), and security manuals and maturity models such as the Information Security Manual (Australian Cyber Security Centre [ACSC], 2025a), from here called "ISM", and Essential Eight (Australian Signals Directorate [ASD], 2023a).

However, as can be concluded from recent Australian National Audit Office (ANAO) audits (2025) and the Commonwealth Cyber Security Posture Report (ASD, 2024a), the full implementation across departments, agencies, and jurisdictions is uneven and still far from completed. This is worrying given the rapid development of new threats in this age of disruption, which are driven by new technologies such as Artificial Intelligence (AI) and Quantum Computing, but also by unexpected geopolitical developments and more evolutionary developments in, for instance, ransomware (ASD, 2025b). In short, we believe that the Australian government needs to accelerate the securing of its information systems in this age of disruption.

The goal of this whitepaper is to identify and examine possible bottlenecks in speeding up the process of strengthening our government systems and to provide pointers for the way forward. The paper is targeted at decision makers responsible for budget and strategic investment and aims to provide concrete tools and recommendations to better prioritise the controls requiring near term implementation.

The remainder of this paper focuses on:

Methodology: Determining gaps in the implementation of security controls and processes in federal and state-level systems in relation to PSPF and the readiness for emerging threats.

Findings: The state of the nation, the importance of uplifting Systems of Government Significance (SoGS) and the identification of systemic barriers and enablers.

Conclusion: Recommendations to build resilience at scale with a forward-looking roadmap.

2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY

On 22 November 2023, the Australian Government's Department of Home Affairs released its 3rd public Cyber Security Strategy (DHA, 2023), The Strategy outlines a roadmap to help realise the Australian Government's vision of being a world leader in cyber security by 2030. It introduces the concept of "shields" as a central framework for protecting the nation against cyber threats. These shields represent layers of coordinated defence designed to strengthen Australia's resilience at every level—individual, organisational, and national. The framework includes six interconnected shields: strong citizens and businesses, safe technology, world-class threat sharing and blocking, protected critical infrastructure, sovereign capability, and resilient region and global leadership. Shield 4 of the Strategy set out a clear ambition: to strengthen the Commonwealth's own cyber resilience. It calls out the importance of implementing the Essential Eight, adopting Zero Trust architectures, and securing new categories of critical systems defined as "Systems of Government Significance."

2. Determining gaps and readiness

2.1 Determining the gaps between the compliance requirements and reality

This paper reviews progress and gaps in the implementation of major policies and frameworks, including the PSPF and the ISM.

It also incorporates insights on funding and budget structure that directly impact investment decisions. A focus on New South Wales (NSW), the Australian Capital Territory (ACT) and Commonwealth agencies is used to illustrate the current situation of system effectiveness to withstand emerging challenges.

To assess the gap between compliance frameworks and operational reality, this project followed a process as laid out in Figure 1. We mapped key security instruments against actual implementation data. The PSPF and related directions from the Department of Home Affairs (DHA) define mandatory protective security obligations, while the ISM and Essential Eight establish technical baselines. Oversight combines strategic planning with independent assurance. The ANAO (2025) audits and the Commonwealth Cyber Security Posture Report (ASD, 2024a) monitor compliance and the implementation of strategies and incident response plans. The centrality of PSPF highlights the need to bridge the gap between compliance and practice. Strategy guides regulation, PSPF sets requirements, ISM/Essential Eight directs technical implementation, and audits track compliance, all strengthening government cyber posture. Imbalances may exist between agency report alignment and PSPF requirements, independent audits, and posture reporting, particularly in Essential Eight maturity and incident reporting.

Recommendations are made around prioritising the uplift of SoGS across governments with centralised services to reduce fragmented management and ensure consistency.

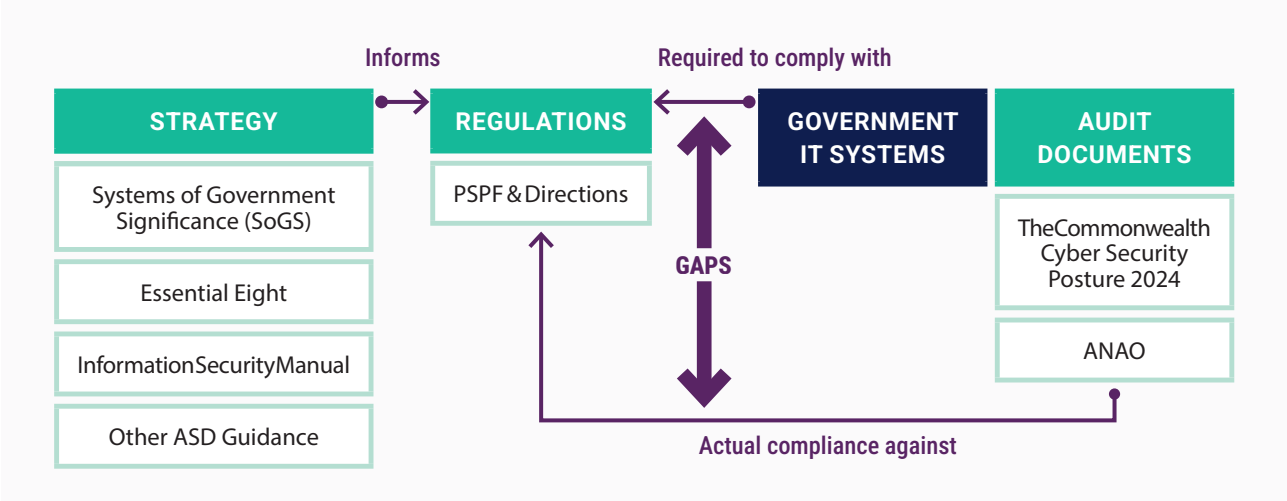


Figure 1: Illustration of the approach and scope of our research.

THE PROTECTIVE SECURITY POLICY FRAMEWORK (PSPF)

The PSPF (Australian Government, 2025) sets mandatory security requirements for all Non-Corporate Commonwealth Entities (NCCEs) and guides broader government adoption of consistent, risk-based protective security. Grounded in the Public Governance and Accountability Act (PGPA) (Australian Government, 2017), it makes security risk management a core agency responsibility. The PSPF is updated annually by the DHA. The 2025 updates introduced strengthened obligations for government agencies, including enhanced cyber security reporting and a mandated Zero Trust culture, clarifying roles and responsibilities, protecting critical assets, maintaining resilience through strategic alignment, and prioritising continuous risk management. New obligations on the use of AI require compliance with the Digital Transformation Agency (DTA) AI policy (2025), security assessments, and stricter procurement standard, especially for foreign owned providers. Agencies must also begin transitioning to approved Post-Quantum Cryptographic (PQC) algorithms under ISM guidance. Additional measures include heightened protection for SoGS, consolidated cyber directives such as mandatory technology asset stocktakes, foreign influence risk assessments, and compulsory participation in ASD's cyber threat intelligence sharing. Existing requirements remain, including achieving Essential Eight Maturity Level 2 to maintain publicsector resilience in a complex threat environment.

2.2 The readiness of government systems for emerging threats

To evaluate the resilience of government systems against emerging threats, our evaluation employed a strategic assessment of readiness across AI-enabled attacks, quantum decryption, and blended cyber-physical threats.

To assess the integration of AI across government services, our evaluation reviewed the operational management and cross-jurisdictional alignment between the PSPF, ASD Guidance, the DTA AI policy (2025), the Australian Public Service AI Plan (Australian Public Service Commission [APSC], 2025) and state-level frameworks. This process focused on how government bodies are navigating the transition from ad-hoc pilots to systemic adoption. The management of AI is currently characterised as a barrier and a transformative enabler.

Regarding the preparation for a quantum future, the PSPF, ASD Guidance and thematic synthesis of the CSIRO 2025 Quantum Readiness Survey (Chhetri et al., 2025) is helpful in revealing how Australian organisations and industries are navigating the transition toward quantum-secure ecosystems. Our analytical process focused on identifying the awareness-action gap, i.e., the disconnect between acknowledgement and action.

THE ESSENTIAL EIGHT

The ASD's Essential Eight (ASD, 2023) are the eight most effective cyber security strategies to help organisations mitigate cyber threats:

- patch applications
- patch operating systems
- use Multi-Factor Authentication (MFA)
- restrict administrative privileges
- control applications
- restrict Microsoft Office macros
- harden user applications
- backup regularly

The framework is underpinned by a Maturity Model that helps organisations systematically improve their cyber security defences. The model consists of three levels, with related sub-controls for each of the controls:

Maturity Level 1 focuses on mitigating basic, opportunistic attacks by implementing fundamental controls in a straightforward manner.

Maturity Level 2 strengthens these controls to address more targeted and sophisticated threats, requiring stricter application and regular maintenance to ensure resilience against adversaries who may actively seek to bypass basic defences.

Maturity Level 3 is designed for organisations facing advanced, persistent threats. This level demands comprehensive, proactive management of security controls, continuous monitoring, and rapid response capabilities to counter skilled attackers who employ adaptive and stealthy techniques.

3. The state of the nation

3.1 Government cyber uplift audits

The annual Commonwealth Cyber Security Posture report (the most recent edition published for 2025) serves as the main and authoritative audit of Commonwealth systems, informing the Australian Parliament on the status and effectiveness of the cyber security measures implemented across the Commonwealth.

It plays a critical role in informing legislative oversight and supporting a clear understanding of the strategies deployed to protect sensitive information and maintain the integrity of Commonwealth systems. Under the PSPF, all NCCEs are required to respond to the survey, while corporate Commonwealth Entities (CCEs) and Commonwealth Companies (CCs) are encouraged to participate. According to the PGPA (Australian Government, 2017) (2013) Flipchart of Commonwealth entities and companies, as of 30 June 2025, the Australian Government comprised 102 NCEs, 74 CCEs and 18 CCs; totalling 194 Australian Government entities. Two entities were excluded from the ASD Survey due to organisational changes.

The information included in the reports is primarily derived from the annual ASD Cyber Security Survey for Commonwealth Entities. Data collected by ASD in the performance of its cyber security function supplements the survey findings, such as metrics gathered by ASD's Cyber Hygiene Improvement Programs (CHIPs) scanning capability of internet-facing systems, which also provide updates on the implementation of effective cyber security standards and protocols. An entity's cyber security posture is considered against the following criteria:

Cyber security hardening: An entity's implementation of cyber security technical mitigations, primarily the Essential Eight mitigation strategies, to reduce the likelihood of an Information and Communications Technology (ICT) system being compromised.

Incident preparedness and response: An entity's readiness to respond to a cyber security incident, and actions when a cyber security incident occurs.

Leadership and planning: An entity's leadership engagement with cyber security and broader cyber security culture.

In 2025, 101 NCEs responded to the ASD survey along with 79 CCEs and CCs, generating an overall completion rate of 94%, the same as 2024. The report shows that, overall, Australian Government entities have established corporate governance mechanisms to understand their security risks and prepare for cyber threats:

82%
HAVE A STRATEGY

82% of entities had a cyber security strategy, an increase from 75% in 2024.

92%
ADDRESSED DISRUPTIONS

92% of entities addressed cyber security disruptions in their business continuity and disaster recovery planning, an increase from 86% in 2024.

91%
PLANNED TO IMPROVE

91% of entities had a planned body of work to improve their cyber security, of which 83% were funded.

90%
HAVE AN INCIDENT RESPONSE PLAN

90% of entities had an incident response plan, an increase from 86% in 2024.

87%
PROVIDE TRAINING

87% of entities provided annual cyber security training to their workforce, an increase from 78% in 2024.

45%
PROVIDE PRIVILEGED USER TRAINING

45% of entities provided annual privileged user training, a decreasee from 51% in 2024.

74%
PERFORM RISK ASSESSMENTS

74% of entities performed supply chain risk assessments for applications, ICT equipment and services.

However, findings also indicate required improvements in some areas. The percentage of entities reporting cyber security incidents to ASD remained low, with 35% of entities indicating that they reported at least half of the cyber security incidents observed on their networks to ASD in 2025, a slight increase from 32% in 2024. ASD has some visibility and telemetry across Government agencies that assist with incident identification. In 2025, ASD notified government entities 223 times of potential malicious cyber activity, an increase from 143 notifications in 2024.

Most significantly, the proportion of government entities that reached overall Maturity Level 2 across the Essential Eight mitigation strategies increased. In 2025, 22% of all entities reached overall Maturity Level 2, up from 15% in 2024, but still below the 25% achieved in 2023. **Despite being required to meet Maturity Level 2 since 2022, agencies have continually struggled to meet this requirement, even when compensating controls are factored in** as illustrated by the adherence patterns in Table 1.

Table 1: Essential Eight Maturity Level 2 Adherence patterns from 2020-2025 (ASD, 2025c; ASD, 2024a; ASD, 2023b; ASD, 2023c)

Essential Eight Maturity Level 2 Adherence

Year	Without Compensating Controls	With Compensating Controls
2020-1	4%	14%
2021-2	11%	19%
2022-3	17%	25%
2023-4	Not reported	15%
2024-5	Not reported	22%

3.2 Uplifting SoGS

In addition to formal security classification frameworks, government departments and agencies typically categorise their systems according to the relative importance and required levels of protection of confidentiality, integrity, and availability.

For instance, common classifications, in increasing levels of importance, may be called Administrative, Business Operational, Business Critical, and Government Critical systems. One would expect that the uplift of the security of these systems is prioritised accordingly, but in practice, and as illustrated further in this white paper, this is consistently not the case.

The Federal Government has recently introduced a new class of systems in the context of PSFP, the so-called SoGS (Burke, 2025). The SoGS are defined as the Australian Government's critical digital functions and systems, identified based on the potential for significant consequences to Australia's economic prosperity, social cohesion or national interest if disrupted. SoGS are closely related to Systems of National Significance (SoNS), a designation introduced through recent amendments to Australia's critical infrastructure framework to recognise assets in the private sector whose compromise or failure could have a material impact on Australia's national security, economy or societal stability.

As part of the PSPF standards, the government has issued a SoGS standard, which details the mandatory cyber security obligations for protecting systems or services that are declared as SoGS. Neither the standard nor the list of systems and services that are declared as SoGS is publicly available. The initiative reflects the government's commitment to have its own critical infrastructure systems match the security requirements that it placed on other critical infrastructure through the *Security of Critical Infrastructure Act 2018* (Critical Infrastructure Security Centre [CISC], 2024) and SoNS listings (CISC, 2025). We can therefore safely assume that SoGS are a cross-section of Business Critical and Government Critical systems based on their confidentiality, availability and integrity requirements.

Given the regulatory and compliance implications associated with SoGS designation, there may be merit in establishing an independent, thirdparty review or assurance mechanism to validate SoGS determinations. Such an approach could strengthen confidence that designations are applied consistently and objectively, reduce the risk of misclassification, and reinforce the credibility of the framework.

One would thus expect that SoGS are the government's top priority in uplifting the protection against crippling cyber-attacks. Our analysis, however, indicates that the security uplift of most SoGS is still in early stages. Though this can be partly explained by the fact that the concept of SoGS is still maturing, we believe that early prioritisation would allow the Federal Government to adapt rapidly, refine governance and cyber security measures progressively. We would also encourage the government to establish effective mechanisms to communicate the requirements SoGS must meet with key technology providers. Clear and consistent engagement would enable vendors to better align their products, services, and support models to assist SoGS in strengthening their cyber security uplift.

We note here that ASD has, for many years, operated whole-of-government cyber uplift initiatives and critical infrastructure uplift programs aimed at raising baseline security maturity across government systems and nationally significant assets (ASD, 2023; ASD, 2024a). Once the SoGS designation and associated system list are fully established, this framework may provide a useful reference point for assessing what has been achieved through earlier ASD-led cyber uplift programs in relation to systems now deemed critical to whole-of-government resilience.

3.3 Systemic barriers and enablers

The various reports from audit committees, such as the Commonwealth Cyber Security Posture reports and ANAO's annual reports, provide snapshots regarding the state of the security of Federal Government IT systems.

Similar auditing processes are defined and executed on state and territory levels for those jurisdictions (Audit Office of New South Wales, 2025; ACT Audit Office, 2020). Our white paper aims to look beyond simply summarising the findings of those reports. Instead, we have tried to look behind those gaps, to identify systemic barriers that complicate or even impede the uplift of those systems, as well as the enabling factors that may accelerate such uplift. In the following subsections, we identify the key barriers and enablers we have found.

3.3.1 The process of auditing itself

Interestingly, one of the barriers identified is the audit process itself. Audits conducted by bodies such as ANAO and ASD typically happen annually, are purely paper based, and provide point-in-time assessments. This represents a rather static approach, and for many systems, that audit is the only formal investigation into their security posture. While additional audit activity may occur between cycles—for example, through Senate Estimates or equivalent state-based processes such as audit hearings—these, too, remain episodic rather than continuous.

While these traditional point-in-time audits provide a useful baseline, they are no longer sufficient for managing cyber risk in modern government environments. Auditors typically validate that controls are in place, i.e., they capture a snapshot of controls on a particular day and tend to be focused on documentation and policy compliance. How systems actually behave, i.e., whether controls operate effectively under real-world conditions, and how threats are evolving in real time is often not reviewed. This can create a false sense of assurance, where an organisation appears "secure on paper" while risk is accumulating unnoticed between audit cycles. This system of audits also reinforces a security culture of seeking compliance (political approval) rather than an ingrained conviction of the need for security deep in the fabric of everyone dealing with government ICT.

Moving to real-time visibility at the agency and department level can help by enabling continuous awareness of assets, configurations, user activity and emerging threats across government systems. Real-time insights allow leaders to detect control failures, misconfigurations and malicious activity as they occur rather than discovering them retrospectively through an audit or worse after an incident. This shift supports more accurate risks prioritisation, faster decision making and stronger accountability at the executive level, transforming cyber assurance from a periodic compliance exercise into an ongoing, operational discipline aligned with how modern threats operate.

We believe that more continuous, real-time monitoring of a whole-of-government security posture is required, particularly for all SoGS. This should sit alongside measures to ensure that each organisation is leveraging real-time, full-stake observability platforms with automated AI-driven detection and response capabilities as well as measures to ensure cyber security is viewed as an operational expenditure (OpEx) rather than a capital expenditure (CapEx) to accelerate their security posture, as discussed below.

3.3.2 Funding process challenges

Government investment approval processes, such as New Policy Proposals (NPP), are critical for ensuring accountability, fiscal discipline, and value for money (Department of Finance, n.d.). However, these processes often create rigid structures and lengthy decision timeframes that conflict with the fast-paced nature of technology and cyber security threats. This tension between rigour and agility is evident across federal, state, and territory

governments. In recent years, this challenge has been amplified by a growing volume of NPPs seeking funding for cyber uplift, which increasingly compete for limited budget capacity and executive attention.

Budget cycles and "gate" processes, designed to enforce policy alignment and delivery assurance, typically assess proposals as discrete, time-bound investments with defined scope and costs. This approach favours well-defined, standalone initiatives such as one-off capital projects. While this ensures financial discipline, it poses challenges for cyber security, which requires continuous, adaptive, and preventative investment to address evolving risks. Departmental gate processes further exacerbate delays by prioritising maturity and certainty, often deferring urgent cyber initiatives until fully developed. Consequently, governments risk reacting to incidents rather than proactively mitigating threats. This dynamic can also skew NPP approval decisions towards systems that are already compromised or experiencing visible failure, as these present a clearer and more immediate justification for investment, compared to preventative uplift of critical but currently functioning networks.

Cyber security priorities shift rapidly due to emerging vulnerabilities and evolving attack methods, demanding flexible acquisition strategies and ongoing investment. Traditional funding models, tied to annual budget cycles and rigid approval gates, struggle to accommodate this need for agility. Governments may need to rethink budget frameworks to enable the timely procurement and deployment of advanced security technologies, ensuring resilience and operational efficiency – particularly as emerging technologies such as AI continues to degrade the cyber threat landscape (ASD, 2024b). **Without such reform, there is a risk that funding continues to be disproportionately directed to "networks on fire"**, rather than being strategically prioritised toward critical networks whose compromise would have systemic or cascading impacts across government and the community.

Another structural challenge lies in the distinction between CapEx and OpEx. Historically, CapEx suited ICT investments like on-premises infrastructure, which depreciated over time. As government entities transition to cloud-based models, there is a systemic shift in financial management from CapEx to OpEx (Department of Treasury and Finance, 2022). This shift clashes with government funding models, as OpEx budgets are more constrained, heavily scrutinised, and subject to annual efficiency measures. Agencies often find it easier to maintain legacy systems under CapEx than adopt modern, more secure services under OpEx, despite better outcomes. Reports highlight that significant effort is spent maintaining outdated environments rather than advancing automated, preventative capabilities.

Further complicating matters, many Software-as-a-Service (SaaS) solutions involve multi-year subscriptions, misaligned with annual budget cycles and procurement frameworks optimised for one-off purchases. Policies such as the efficiency dividend and offset rule intensify these challenges by eroding operating budgets and requiring new investments to be offset by savings elsewhere. These constraints can lead agencies to defer upgrades or reduce scope, undermining efforts to build long-term cyber resilience. For critical networks, these constraints can delay necessary uplift until risk has already materialised, reinforcing a reactive rather than preventative funding posture (more on this below).

In short, there is an opportunity to evolve budget and investment frameworks, so they better support modern cyber security needs. This is not about abandoning fiscal discipline, but about refining existing processes to better reflect the lifecycle, operational and strategic characteristics of digital and cyber capability. As cyber security becomes increasingly central to government operations and public confidence, aligning financial frameworks with these realities will help governments at all levels continue to deliver secure, trusted and resilient services in an increasingly contested digital environment. This includes ensuring that NPP assessment and approval processes explicitly account for the criticality of networks, not solely the immediacy of compromise, when determining investment priority.

3.3.3 Risk-based prioritisation of cyber upgrades

Given the government's current auditing and financing processes as described above (shared across federal, state and territory governments), the choices being made in terms of which systems to be upgraded when and how are often more determined by these processes than by industry state-of-the-art threat-modelling procedures and related risk assessments. As a result, risk-based prioritisation can be distorted by funding and approval mechanisms that favour incident-driven remediation and compliance with controls, over risk-based proactive investment in critical systems that have not yet failed. Many standardised methods for cyber risk assessment and management exist, including Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts et al., 1999) and National Institute of Standards and Technology's Risk Management Framework (NIST RMF) (National Institute of Standards and Technology, 2018).

Threat modelling is an integral part of these methods and includes the planned activity for identifying and assessing cyber threats and mitigation strategies. Root Cause Analysis (RCA) is key component of threat modelling as it acts as bridge between proactive security design and reactive incident response. RCA analyses why a vulnerability or security occurred by identifying the underlying causes of failures rather than just treating symptoms, as such solidifying future defence strategies (Stouffer, 2019) (Cichonski, 2012). Various powerful tools exist to support the hunt for threats and perform RCA, some of them as open source as supported by AI (see, for example Cisco's Foundation-sec-8b Security Small Language Model (Singer, 2025)).

The outcome of a cyber risk assessment is a list of identified cyber threats, including 1) their likelihood of occurring, 2) the impact such a breach would cause, 3) costs (CapEx and OpEx) and duration for mitigation. These properties subsequently enable the prioritisation of threats, and that should be the main input for decision-making around which threats should be mitigated first. For this approach to be effective, funding decisions must be explicitly aligned to these risk outcomes, ensuring that critical networks are prioritised for investment even when no active comprise has yet occurred.

The designation of SoGS is likely to help with prioritisation and enable targeted investment and oversight of critical systems, strengthening resilience and reducing exposure to service outages, cyber threats, and operational breakdowns. Hence, the threat modelling of SoGS as a strategic priority will assist the government in focusing resources where failure or outage would have the most detrimental impact, to ensure resilience, continuity and long-term sustainability across the public sector. **Overlaying SoGS designations into funding and approval processes provides a practical mechanism to rebalance investment decisions toward critical networks** as a matter of strategic risk, rather than waiting for those systems to become "the next incident".

3.3.4 Appropriateness of Essential Eight

The Essential Eight has become, somewhat ironically, a source of challenge in the context of government cyber security uplift. Originally conceived as a small set of practical, prioritised actions to improve baseline cyber hygiene, the Essential Eight has evolved into a formal maturity model with expanding requirements. It is now mandated across Federal Government via the PSPF and plays a central role in audit and assurance processes (Australian Government, 2025; Australian National Audit Office [ANAO], 2025).

Despite this mandate—and despite government investment in multiple initiatives designed to support Essential Eight uplift—many agencies have struggled to meet the required maturity levels (ASD, 2024a). This raises important questions about whether the Essential Eight, as currently applied, represents the right standard for government, and whether agencies are being provided with sufficient funding, capability, and structural support to achieve compliance in complex and resource-constrained environments. Further the ongoing evolution of Essential Eight controls, while necessary to address emerging threats, may at times impact the sequencing and timing of agency

uplift activities, particularly where implementation plans are aligned to earlier control interpretations.

Conversely where agencies do achieve an agreed maturity target, there is a risk that Essential Eight maturity levels are treated as a defined endpoint rather than as part of a continuous risk management cycle. This reflects, in part, an organisational mindset that equates attainment of a specified maturity level with acceptable residual risk, leading to a temporary deprioritisation of security investment once a target level (for example, Maturity Level 1 or 2) has been reached.

The strong emphasis placed on Essential Eight compliance within audit processes has also had unintended consequences. In some cases, agencies have become overly focused on meeting prescribed control requirements at the expense of broader, risk-based security management practices. This outcome can reinforce a compliance-driven view of cyber security maturity, rather than one that recognises cyber risk as persistent, evolving, and requiring sustained management over time. This compliance-driven approach can obscure more material risks and reduce flexibility in addressing emerging threats or agency-specific vulnerabilities (ANAO, 2025).

In addition, the Essential Eight has been criticised for its historical focus on traditional on-premises environments and for insufficiently addressing key aspects of modern cloud and SaaS operating models (ASD, 2023a; Zacks, 2024). Gaps have also been identified in areas such as identity security beyond MFA, mitigations against credential-based attacks, including brute force techniques and crucial protection and hardening of network infrastructure.

ASD has consistently emphasised that the Essential Eight is intended to complement—not replace—a broader suite of security controls, frameworks, and risk management practices (ASD, 2023a). It is in this context that achieving sustained government cyber uplift may require not only re-centring the Essential Eight within a holistic, risk-based security model, but also undertaking a broader review of the framework itself. Such a review could identify structural and operational blockers preventing agencies from achieving Maturity Level 2, assess alignment with contemporary architectures and threat models, and consider if additional guidance, flexibility, or targeted investment may be required to support consistent uplift across government.

3.3.5 Legacy environments

LEGACY AND END-OF-LIFE ICT

Legacy ICT refers to ICT systems that remain in operational use despite having reached the end of their lifecycle, where they are no longer suitable for upgrade or remediation due to technological or commercial constraints, or are no longer supported by the supplier or an ICT third party service provider. In this paper, End of Life (EoL) is used to include End of Support (EoS) and End of Security Support (EoSS), referring to technologies for which suppliers have ceased providing security patches, fixes, updates, or technical support, or that can no longer be practically extended. While all EoL systems are legacy, not all legacy systems are EoL; however, legacy systems that fall within the EoL category typically present elevated cyber security risk due to the absence of ongoing security maintenance.

Legacy ICT environments are significantly more vulnerable to cyberattacks and often prevent agencies from implementing enhanced security controls (e.g., for achieving Essential Eight Maturity Level 2), with risks escalating sharply as systems reach EoL. While legacy systems may continue to operate as designed, EoL technology is no longer supported by vendors and cannot be adequately patched, monitored, or secured. Malicious actors can exploit these weaknesses to compromise EoL systems and use them as a foothold to access more modern components of the broader IT environment. As a result, security risks multiply: vulnerabilities accumulate, detection and response capabilities deteriorate, and recovery from cyber incidents becomes slower and more complex. For government agencies, the speed at which systems can be restored following a cyber incident is critical. In addition, many of our legacy ICT systems are not resilient enough to withstand emerging digital

and cyber threats, including AI-enabled attacks and cannot be PQC ready or in other words, implement PQC algorithms.

While there is no consolidated data to quantify the scale of legacy ICT across Australian governments, reporting from the United Kingdom (UK) suggests that the number of legacy systems is increasing across government, with a growing portion assessed as high risk due to their fragility and security exposure. In 2024, 288 legacy ICT systems were identified across UK Government Department, with over 1 in 4 of those "red-rated" with a high likelihood and impact of operation and security risks occurring (National Audit Office, 2025). In the United States (U.S.), 80% of federal IT spending goes to operating and maintaining existing—often legacy — systems (WPI Strategy, 2025).

The 2024 Commonwealth Cyber Security Posture report specifically calls out that **legacy ICT presents significant and enduring risks to the cyber security posture of Australian Government** – preventing many entities achieving Maturity Level 2. In 2025, 59% of organisations indicated that the use of legacy technologies had impacted their ability to implement the Essential Eight, a decrease from 71% in 2024. The most significant reasons entities reported for continuing to use legacy ICT include insufficient dedicated fund-ing (34%) and lack of viable replacements (18%), followed by lack of prioritisation (16%) and insufficient skilled personnel (2%). Other or unspecified reasons accounted for 30%. ASD con-tinues to provide guidance on managing the risks associated with legacy IT, but these chal-lenges remain a significant barrier to achieving higher levels of cyber security maturity across government entities.

The challenge of updating and securing legacy systems should be considered in the context of the ever-increasing overall national cost of ICT and cyber investments (Gartner, 2024). In here, the proportion of spending needed to maintain legacy ICT systems is a significant issue. In 2023, the U.S. federal government spent $100 billion on IT and cyber-related investments. Estimates are that $80 billion of this will be spent on operating and maintaining existing systems including legacy systems, an increase of 12% on 2021 spending (WPI Strategy, 2025).

The costs of maintaining aging technology should focus policymakers on whether they are making the right investment decisions. However, this decision-making ability is often clouded by the earlier-mentioned funding challenges: public sector ICT projects tend to focus on CapEx, with maintenance costs dealt with as OpEx. With continued pressure on finding savings in public sector budgets, that encourages a tendency towards short-term savings on operating costs. This forgoes the benefits of managing technology and stores up more costly, long-term maintenance. And so, paradoxically, this will eventually lead to an increase in the proportion of spending going on maintenance, rather than modernisation or enhancement. In this way the cost of maintaining aging technology can be seen as two-fold: a "technical debt" paid by having to manage outdated devices and software, and a "tax" against deploying enhancements or innovations.

These findings highlight key barriers to modernising ICT infrastructure. Governments should adopt a more proactive and coordinated approach to managing legacy ICT, particularly EoL technology across SoGS. At a minimum, all agencies should be accountable for maintaining live technology asset registers that identify legacy and EoL ICT. Current requirements focus on maintaining visibility into internet-facing assets only. But to manage systemic risk, this should be extended to live asset registers that capture the full scope of legacy ICT, supported by standardised lifecycle management and risk assessment requirements. This would enable early identification of assets approaching EoL and informed decisions on replacement or active risk management.

In parallel, governments should strengthen policy, procurement, funding, and regulatory levers to reduce systemic EoL ICT risk. Procurement should be used as a preventative control, requiring vendors and service providers to disclose product lifecycles (including End of Sale and EoL milestones) committing to ongoing security patching and provide defined transition or exit pathways once technologies become unsupported. Reforming ICT investment and procurement models to favour

lifecycle managed, service-based models could help redirect spending from technical debt towards remediation and replacement. These changes should be complemented by piloting targeted "rip and replace" funding for the highest risk EoL systems. Incident reporting regimes should capture the role of EoL technology to improve transparency and inform risk-based responses. Finally, governments should explore how emerging technologies, including AI enabled testing and deployment tools, can safely reduce patching delays and support the protection or isolation of systems that cannot be immediately updated or replaced.

3.3.6 Planning for new cyber threats around AI

APSC (2025) highlights that APS agencies have already integrated AI to embrace advances in technology, within a policy framework for responsible AI. Agencies are increasingly using AI transparency statements to explain how and why they apply AI in their work, helping build public understanding and trust. The report includes 12 case studies that illustrate how APS agencies are adopting AI across a wide range of functions, including service delivery, compliance and fraud detection, law enforcement and security, scientific research, and internal corporate and enabling services.

Despite AI adoption growing in the APS, there are still gaps in its risk management, ethical assessment, and governance across states and territories. Although the AI readiness of Australia's government systems is advancing, it remains at a pivotal point between strong policy ambition and uneven operational maturity. Recent federal strategies and governance frameworks now require agencies to use risk-based approaches, including impact assessments and alignment with the National AI Plan and the APS AI Action Plan, which emphasise trust, capability uplift, and responsible deployment.

Yet the main challenge lies in putting policy into practice. Operational capability varies widely across agencies. Demand for AI often exceeds the ability to manage its security risks. The Cisco AI Readiness Index 2025 (Cisco, 2025) shows that although most organisations plan to deploy AI agents, only a minority consider themselves fully equipped to secure them. Weak governance, limited model visibility, and immature access controls create significant risks to security and public trust. In addition, fragmented and poorly governed data environments represent a major impediment to both deriving value from AI and securing its use, as inconsistent data quality, lineage, and access controls undermine model reliability, increase exposure to misuse, and complicate effective risk management. And while the PSPF reinforces secure AI adoption, its mandates apply only to NCCEs, leaving gaps across other jurisdictions. At the same time, there has been limited focus on the risks of not deploying AI quickly enough to counter increasingly AI enabled cyber threats.

Legacy infrastructure poses another major challenge. Only a third of organisations believe their systems can scale for AI, and accumulating "AI infrastructure debt"—outdated systems, fragmented data, and under-resourced security—threatens the effectiveness and safety of AI adoption. Without modernised ICT foundations, governments risk undermining both capability and security as AI use accelerates.

Government therefore needs secure-by-design AI, strong guardrails, and alignment with broader cyber frameworks. The recently released guidance on Australian Government use of public generative AI tools provides the initial tools for securing the use of AI by the APS and should be executed immediately, but should also be updated regularly, as more knowledge about the threats against AI is obtained (DTA 2025). The government should also investigate the use of AI as an enabler for improving the cyber security of government systems, for instance, in leveraging AI for predictive and autonomous incident detection and response.

3.3.7 Planning for a post-quantum future

On 22 September 2025, ASD released "Planning for Post Quantum Cryptography" (2025a) guidance which assessed that a first, practical cryptographically relevant quantum computer

(CRQC) will become available by the end of 2030, as illustrated by Figure 2. Such a CRQC will primarily threaten the security of systems that rely on traditional asymmetric cryptographic algorithms and will also have implications, albeit to a lesser extent, for symmetric encryption and hashing. Notably, the security of both authentication mechanisms and data in transit will be vulnerable.

Beyond the technical implications, the quantum threat should be understood as a systemic risk rather than solely a cryptographic concern. At scale, the compromise of cryptographic trust has the potential to create cascading failures across authentication systems, service assurance platforms, network control planes, and secure orchestration layers, with broader consequences for operational continuity, public trust, and national and economic security.

While the awareness of the need for PQC is relatively high in our government departments and agencies, this awareness has not yet fully shifted into organisational engagement and strategic integration. Most agencies acknowledge the risks posed by quantum-enabled attacks, but practical engagement remains restricted due to uncertainty, low prioritisation and a lack of internal expertise, as uncovered by a recent CSIRO report (Chhetri et al., 2025). This gap between acknowledgement and action is further reinforced by the cost and complexity of cryptographic change, particularly in large, legacy-heavy environments, which further reinforces the difficulty for organisations to prioritise without sufficient support and guidance.

In addition, the risk of harvest now, decrypt later (HNDL) attacks heightens the urgency of early preparation. Sensitive and regulated data intercepted today may remain vulnerable to future decryption once cryptographically relevant quantum capabilities become available, creating long-term confidentiality, legal, and regulatory exposure for government entities.

In this context, quantum safe migration should be viewed not merely as a technical exercise focused on replacing cryptographic algorithms, but as a longterm strategic transformation program embedded within broader digital modernisation, trust governance, and enterprise risk management initiatives. Framing migration in this way reinforces

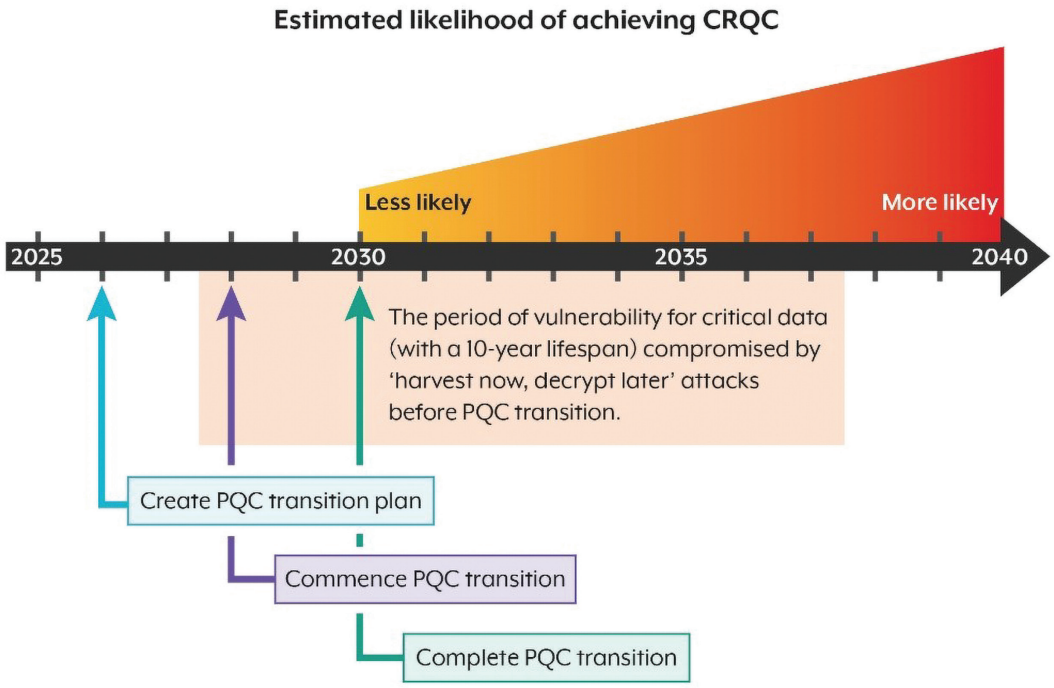


Figure 2: Timeline of CRQC likelihood (2025–2040) with a gradient likelihood bar. Figure from ACSC (2025b).

its role in strengthening systemic resilience, rather than treating it as a standalone cryptographic uplift.

While we note that the Commonwealth has updated the PSPF to require all NCCEs to be PQC ready, we recommend that the government consider expanding this requirement to all Commonwealth entities. Further efforts are also needed to actively promote this guidance among key stakeholders and to develop government-specific materials to ensure awareness and understanding (ANAO, 2024; ASD, 2023c). Noting that ASD suggest by the end of 2026, organisations should have a refined plan for their transition preparation should start as soon as practically possible, especially for SoGS, while also cautioning against premature, potentially abortive efforts given the evolving solution space.

The government should complement the policy-level guidance with implementation pathways—including reference architectures, algorithm transition frameworks, and practical adoption models that can help large enterprises and service providers operationalise the guidance at scale.

ASD's Guidance represents a welcome first step in preparing for the challenges posed by quantum computing (2025a), which includes the creation of Cryptographic Bill of Materials (CBOMs). However, cryptographic discovery alone does not equate to systemlevel readiness. Organisations must also understand how cryptographic dependencies are embedded across architectures, supply chains, and operational processes, and how changes to cryptographic primitives may affect interoperability, performance, and service assurance.

CRYPTOGRAPHIC BILL OF MATERIALS (CBOMS)

A CBOM is a detailed inventory of all cryptographic components (algorithms, keys, certificates, libraries, protocols) within a system. Particularly the deployments of asymmetric cryptography require attention as this type of cryptography is most vulnerable. This is not limited to data transmission but also includes asymmetric cryptography options in hardware that can expose the integrity of, for example, network devices.

Guidance is also needed on how to prioritise efforts in addressing quantum threats and how to assess their overall readiness beyond product-level implementation. We here refer to the earlier mentioned cyber security risk management methods and threat modelling procedures. These should now include evaluating systemic protection strategies that holistically address quantum-related risks.

As agencies implement ASD guidance, cryptographic agility should be treated as a core architectural and governance principle, while also supporting Zero Trust adoption and secure by design system evolution. Effective implementation will depend on strong governance and clear ownership, including executive accountability for quantum-related risk, defined decision-making and escalation pathways, and integration of PQC considerations into existing cyber security, technology, and enterprise risk forums. Treating PQC solely as a technical risk underestimating its enterprise-wide impact and slowing progress.

To maintain transparency and momentum, agencies should track progress and residual quantum risk using indicators such as readiness milestones, coverage of high-value data and systems, and exposure of critical dependencies. Given the cross-cutting nature of cryptography, delivery will require coordinated engagement across ICT, cyber security, risk, legal, procurement, and business functions.

For these reasons, **the government should consider positioning the quantum threat not just as a cryptographic concern, but rather as a systemic risk** to national and economic security, digital resilience and trust, and operational continuity.

3.3.8 Fragmented uplift across different entities on the federal and state levels

Due to the fragmented management of services and cyber security policy across federal, state and territory governments, their coordination remains limited, contributing to inconsistent cyber uplift across jurisdictions. This is reflected in the uneven implementation of essential security frameworks such as the PSPF and the Essential Eight. The federal government has proven to lead

nationally in cyber compliance and preparedness to emerging technologies, including AI and quantum computing, whereas other jurisdictions present substantial progress or lag, creating gaps in baseline security performance and exposing systematic vulnerabilities.

A further complicating factor in many states and territories is the reliance on shared services models, where multiple entities depend on common ICT and security service providers. In such arrangements, individual agencies' cyber maturity is inherently constrained by the security posture, investment priorities, and uplift pace of the shared service provider, limiting their ability to independently improve resilience. The absence of a unified uplift approach suggests that national cyber preparedness depends heavily on the maturity of states and territories. We illustrate this below with two examples: NSW and ACT.

A review of NSW's Cyber Security Policy (CSP) by the Department of Customer Service (2024) and the Cyber Security Insights NSW report by the Audit Office of NSW (2025) highlights significant implementation challenges and uneven maturity across agencies. CSP is a comprehensive framework aligned with the PSPF, and just like PSPF is not mandatory to non-NCCEs, the CSP is not mandatory for state-owned corporations, local governments, universities, or non-governmental organisations, leading to inconsistency. A difference with CSP is that, under CSP, agencies must implement the Essential Eight controls at a minimum Level 1 maturity, whereas PSPF requires Level 2.

NSW designated 2023–24 as a baseline year, meaning full compliance was not expected; however, findings reveal concerning gaps. The Cyber Security Insights report (Audit Office of New South Wales, 2025) shows that many agencies failed to achieve even Level 1 maturity for critical controls such as application control, patching, and administrative privilege restrictions, leaving fundamental vulnerabilities. Risk reporting underscores the severity: 27 of 66 agencies reported 152 significant, high, or extreme cyber risks. Compliance was particularly weak in the 'Protect' domain, where only 31% of mandatory requirements were met.

Common reasons for non-compliance include ongoing or planned uplift programs, budget constraints, lack of formalised processes, and insufficient resources (Audit Office of New South Wales, 2025). Additionally, systemic issues such as fragmented compliance and limited progress despite clear policy direction persist. Overall, NSW faces substantial gaps in cyber resilience, with agencies struggling to meet baseline expectations, exposing the state to heightened risk and underscoring the need for stronger enforcement, resourcing, and capability uplift.

The ACT Government's cyber posture is shaped by the ACT Protective Security Framework (PSF) (Justice and Community Safety Directorate [JACSD], 2025a), Core Practice Standards (CPS) (JACSD, 2025b), Cyber Security Policy v3.5 (ACT Government, 2025), and the Data Security Report 2020 (ACT Audit Office, 2020). Unlike NSW, the ACT's approach is governance-focused, prioritising risk management and policy alignment over prescriptive technical controls. Compliance is encouraged rather than mandated, resulting in uneven uplift across agencies. The ACT Audit Office's report (2020) noted strong alignment with ISM and ACT PSF.

A key strength is ACT's forward-looking stance on emerging threats, particularly quantum risk. The ACT Government's Cyber Security Policy (2025) introduced concepts such as CRQC and CBOMs, requiring agencies to document cryptographic assets for future resilience. While budget constraints remain a challenge, ACT demonstrates strategic readiness in AI and quantum domains, framing uplift within governance structures rather than technical mandates. Challenges that the ACT is currently acting on include fragmentation of responsibilities between ICT teams, cyber teams, and the Justice and Community Safety team (the latter being responsible for PSF), and the need for new budgeting procedures that are more suitable for cyber security investments.

A final example of fragmented approaches in securing government systems concerns the practice of vendors to have their solutions

assessed by third-party Infosec Registered Assessors Program (IRAP) assessors. IRAP is managed by ASD and provides organisations with access to qualified, independent, certified professionals who conduct security assessments of ICT systems or products. Many vendors pursue IRAP assessments to demonstrate that their services can meet federal government standards, providing assurance to agencies and enabling them to sell their solutions to the government market. While it has become routine for federal government agencies to ask vendors for product IRAP assessments as part of their procurement process, this has not occurred at the state and territory level.

Taken together, these cases illustrate how fragmented governance, inconsistent policy mandates, and uneven resource allocation across jurisdictions have created structural gaps in Australia's cyber uplift. While the Commonwealth sets a strong baseline through the PSPF and emerging requirements for SoGS, the varying maturity, compliance expectations, and investment models across states and territories mean that national resilience is only as strong as its weakest link. Addressing this fragmentation requires a shift toward more unified, risk-based and coordinated uplift—supported by mandated minimum standards, consistent reporting requirements, and shared uplift mechanisms across all levels of government. Doing so directly aligns with our recommendations to close the policy-to-practice gap, reduce jurisdictional variability, and strengthen national preparedness through continuous assurance, centralised guidance, and prioritised uplift of critical systems.

3.3.9 Low rates of reporting incidents to ASD

The Commonwealth Cyber Security Posture (ASD, 2025c) highlighted significant gaps in incident reporting, with 35% of entities indicating that they reported at least half of the cyber incidents detected on their networks to ASD, an increase from 32% in 2024. While this reporting rate is significantly higher than that of many industry sectors, the remaining under-reporting reveals critical gaps. It indicates low situational awareness and a likely lack of real-time monitoring. Furthermore, it highlights that without consistent incident reporting, the ability to coordinate timely and effective responses is severely compromised. **Higher levels of reporting would not only provide ASD with more realistic information about the security posture of Australia's IT systems but would also enable ASD to provide better advice** and help with incident response when government systems are confronted with cyber incidents.

From July 2024, reporting requirements have materially strengthened, with the introduction of a mandatory obligation for NCCEs to report all cyber incidents to ASD, subsequently formalised in the 2025 update to the PSPF. These reforms are expected to significantly improve reporting coverage and consistency over time, addressing many of the shortcomings identified in earlier assessments. PSPF/ASD reporting obligations now apply to all NCEs, CCEs are not universally mandated, and states/territories are not covered by a single nationwide mandatory ASD reporting requirement (ASD, 2024a; Australian Government, 2025). Going forward the government may wish to consider expanding mandatory reporting requirements to apply to all government agencies.

In parallel, the expansion of ASD's Cyber Threat Intelligence Sharing (CTIS) service represents a critical uplift in national cyber situational awareness (Defence Ministers, 2024). CTIS is a two-way sharing platform that enables government and industry partners to continuously receive and share information about malicious cyber activity. In late 2024, ASD delivered a new in-house CTIS platform, and by June 2025, 35 government entities are part of the CTIS program with 18 additional entities in the pipeline to connect. Both Microsoft and Splunk have developed plugins for their respective security operations platforms, which are strong enablers for ASD to build online resilience and counter cyber threats. Under the updated PSPF, all NCCEs are now required to connect to CTIS, improving visibility of emerging threats and enabling faster, more coordinated responses. Consideration should be given to expanding CTIS participation to all Commonwealth entities, and to encouraging or incentivising state and territory

governments to connect to the platform and report all cyber incidents to ASD, to further strengthen cross-jurisdictional threat awareness and collective defence.

3.3.10 Workforce challenges

Upgrading the government system's security posture is frequently hampered not only by technical challenges, but also by a structural "capability ceiling". This ceiling, driven largely by the acute shortage in the cyber workforce, serves as a restrictive barrier that limits the efficacy of all other technical uplifts and negatively impacts the mitigation of cyber risks in the long term.

Australia faces a significant cyber security workforce shortage, with demand for skilled professionals continuing to outpace supply. The Australian Computer Society's (2025) Digital Pulse 2025 report notes that while Australia's technology workforce exceeded 1 million in 2024, demand is projected to reach 1.3 million, and the shortage of cyber security talent is expected to double by 2030. Government reports highlight sustained demand in ICT security roles and recommend upskilling across all levels—from entry-level to executive positions. However, attracting, retaining, and upskilling cyber talent remains a challenge for the government, as private sector salaries are generally more competitive (DHA, 2025). Compounding this issue, Salesforce (2025) reveals widespread gaps in training for emerging technologies such as AI, with only 41% of workers reporting workplace preparedness. Senior leaders also face "education fatigue," as evolving cyber threats demand continuous upskilling, making it increasingly difficult to maintain relevant competencies.

Workforce readiness is a critical enabler for accelerated uplifting of the security posture of government systems, particularly with the advance of new technologies such as AI. Unfortunately, most organisations lack clear plans for reskilling, role redesign, and establishing new governance and oversight functions for AI. Only leading organisations invest in change management and AI-specific skills early. Governments must similarly plan for capability uplift, workforce transition, and responsible use of training, particularly as AI agents increasingly augment or automate public sector tasks.

In addition, there is a growing need to uplift baseline cyber and ICT literacy across non-technical disciplines that play critical assurance and oversight roles, including legal, audit, risk, finance, and compliance functions. It is important that these roles maintain a foundational level of ICT and cyber security literacy to reduce dependence on agency ICT teams and strengthen governance, assurance, and risk-based decision-making. This highlights an opportunity to embed minimum ICT and cyber security competencies within relevant professional qualifications and to require periodic refresher training to maintain currency, ensuring that cyber risk is understood and assessed consistently across disciplines.

Beyond immediate capability gaps, government also needs a more systematic understanding of its long-term cyber and digital skills requirements. The skills needed to manage today's ICT and cyber environments will not necessarily align with those required to secure future architectures shaped by cloud, AI, quantum-resilient cryptography, and increasing automation.

Without forward-looking workforce planning, there is a risk that training and recruitment efforts remain reactive, reinforcing cyclical skills shortages rather than building sustained capability.

Universities have a role to play in this urgent need for training and upskilling of the professional workforce and should consider if the traditional offerings of graduate degrees are fit for purpose. Educational innovation may be needed in the form of short courses, online offerings, self-paced courses, and micro-credentialling, leading the way for the entire education sector in providing tailored training and upskilling suited to the demands of a new society.

4. Conclusions and recommendations

We conclude that the approach to securing government ICT systems in Australia must move from audit-driven policy compliance prioritisation and investment to more continuous, centralised, and risk-prioritised actions, aligned across federal, state and territory governments, to withstand the accelerating threats.

Given the geo-strategic environment and as we enter into Horizon Two of the Cyber Security Strategy, this report settles on the following recommendations.

01

RECOMMENDATION 1

Close the policy-to-practice gap

The Australian Government should lead a coordinated, time-bound uplift of critical systems across federal, states and territories, through practical implementation pathways for PSPF as well as AI and PQC readiness, a central OpEx-suitable funding mechanism, and mandated reporting throughout the year to close the policy-to-practice gap at scale.

02

RECOMMENDATION 2

Augment point-in-time audits with real-time visibility and continuous assurance to improve responsiveness to emerging threats

Organisations should continuously monitor the operational effectiveness of controls, as such complementing periodic compliance with continuous assurance. Transition cyber assurance from periodic, retrospective audits to include continuous, real-time visibility at the agency and departmental levels.

03

RECOMMENDATION 3

Make the uplifting of SoGS a strategic priority

Making the uplifting of SoGS a strategic priority will assist the government in focusing resources where failure or outage would have the most detrimental impact, to ensure resilience, continuity and long-term sustainability across the public sector. Early prioritisation would allow the government to adapt rapidly, refine governance and cyber security measures progressively.

04

RECOMMENDATION 4

Strengthen the messaging surrounding the requirements of SoGS

The government should establish effective mechanisms to communicate the requirements that SoGS must meet with key technology providers. Clear and consistent engagement would enable vendors to better alignment to assist SoGS in strengthening their cyber security uplift.

05

RECOMMENDATION 5

Review NPP and budgeting methodologies to support preventative, risk-based cyber investment

Funding and approval mechanisms should be adapted and aligned to prioritise investments based on assessed risk and system criticality, rather than favouring incident driven remediation, or visibly failing systems.

06

RECOMMENDATION 6

Introduce greater flexibility for OpEx-based and multi-year cyber investments

Align fiscal frameworks with ongoing cyber security requirements by enabling sustainable OpEx-based funding models. Governments should review the current investment frameworks to ensure they are fit for purpose in supporting modern cyber security resilience and operational efficiency. Funding models should better accommodate the operational nature of cyber security, including cloud, SaaS, monitoring, and detection capabilities, to reduce reliance on CapEx-centric decision making. Where appropriate, encourage investments in ongoing cyber activities to be proposed and granted as OpEx instead of CapEx to accelerate modern security posture.

07

RECOMMENDATION 7

Drive cyber defence through a risk management lens

Prioritise controls and funding based on organisational context and value, threat exposure, asset criticality, impact and RCA, and let those priorities determine the pathway toward compliance obligations. Controls should be implemented and prioritised based on threat, consequence, and exposure—not solely to satisfy audit requirements. Such approach would then also pave the way to move from encouraged compliance with an essential policy framework toward mandated compliance across the board.

08

RECOMMENDATION 8

Review the Essential Eight for its suitability for government systems

Conduct an independent review of the Essential Eight to assess its suitability for modern day government ICT environments, including cloud native, SaaS, identity-centric and highly federated architectures, as well as emerging threats, including AI-enabled attacks. The review should identify structural and operational blockers preventing agencies from achieving Maturity Level 2, consider if additional guidance, flexibility, or targeted investment may be required to support consistent uplift across government.

09

RECOMMENDATION 9

Accelerate coordinated action on legacy (EoL) ICT, particularly across SoGS

Governments should adopt a more proactive and coordinated approach to managing legacy technology, particularly across SoGS. Agencies should be required to maintain live technology asset registers identifying legacy and EoL systems, supported by wholeofgovernment prioritisation and targeted replacement or isolation strategies. Capture the role of EoL technology in Incident reporting to improve transparency and inform risk-based responses.

10

RECOMMENDATION 10

Introduce targeted funding mechanisms for high risk legacy systems (EoL) replacement and strengthen legacy retirement levers

Introduce targeted funding mechanisms for high-risk legacy system replacement and strengthen legacy retirement levers. Government should establish dedicated “rip-and-replace” or technical-debt-reduction funding for the highest-risk EoL systems that materially inhibit cyber uplift and resilience. Procurement, regulatory, and targeted investment mechanisms should be used in concert to accelerate the retirement of high-risk legacy systems and reduce systemic EoL-related risk. This includes embedding minimum cyber hygiene, patching, and support obligations into vendor contracts, and promoting ICT investment models that shift funding away from servicing technical debt and toward maintenance, remediation, and replacement. Where immediate replacement is not feasible, governments should explore the use of new tools—including open-source and AI-enabled testing and deployment capabilities—to reduce patching delays and to isolate or shield legacy systems pending retirement.

11

RECOMMENDATION 11

Harness AI to strengthen cyber defence

Implement secure by design AI and leverage defensive AI capabilities to enhance system monitoring, detection and response. The recently released guidance on Australian Government use of public generative AI tools should be executed immediately, but should also be updated regularly, as more knowledge about the threats against AI is obtained. The government should also investigate the use of AI as an enabler for improving cyber security of government systems, for instance, in observability platforms.

12

RECOMMENDATION 12

Treat quantum computing as a systemic risk and make the transition to PQC a long-term strategy

Position PQC uplift as a whole-of-government resilience priority with clear migration pathways, especially for complex and interconnected systems. Plan PQC adoption as a phased, multiyear transformation of government cryptographic foundations, rather than a discrete technical update. Treat ASD's 'Planning for Post-Quantum Cryptography' framework as a first step, but complement policy guidance with practical implementation pathways, particularly for SoGS.

13

RECOMMENDATION 13

Reduce jurisdictional variability

To support a more seamless security uplift, it would be beneficial to work toward common security goals across federal and state lines. Leveraging incentives can help bridge gaps, ensuring that all entities can progress together effectively. The absence of a unified approach leaves national preparedness reliant on jurisdictional maturity. And in a system of government systems, the system will be as secure as its weakest link.

14

RECOMMENDATION 14

Expand cyber incident reporting requirements to ASD for all government entities

Incident reporting obligations should be extended beyond NCCEs to include all Commonwealth entities, improving national situational awareness and coordinated response capability. Work with states and territories to raise awareness of and incentivise reporting.

15

RECOMMENDATION 15

Address the cyber skills gap to create, attract, and retain a cyber workforce

Invest in targeted workforce uplift, leadership capability development and retention strategies to sustain secure digital operations. Comprehensive training programs, targeted incentives, and sustained government support are particularly urgent to keep pace with rapid AI adoption. Stimulate educational innovation in the form of short courses, online offerings, self-paced courses, and micro-credentialling.

Acknowledgements

The development of this white paper has been greatly strengthened by the insights, expertise and generous support of the many contributors who engaged with us throughout its preparation. We are deeply grateful to the government officials from ASD, the DHA, ACT Government and industry specialists from Cisco Systems, Inc., who provided thoughtful feedback, shared valuable operational perspectives, and challenged our assumptions in ways that helped sharpen and refine our analysis. While this paper has benefited greatly from the time, expertise, and collaboration of all involved, the views, interpretations and recommendations expressed herein are solely those of the authors. They do not necessarily reflect the positions or perspectives of any organisation or individual who contributed to the review process.

Contact

For further information regarding this white paper, its analysis or recommendations, please contact:

NIIN National Industry Innovation Network

National Industry Innovation Network: communications@niin.com.au

Innovation Central Canberra

A collaboration led by cisco

Innovation Central Canberra: innovationcentral@canberra.edu.au

References

ACT Audit Office. (2020). Data security (Report No. 3/2020). https://www.audit.act.gov.au/__data/assets/pdf_file/0007/1561219/Report-No.-3-of-2020-Data-Security.pdf.

ACT Government. (2025). ACT Government Cyber Security Policy (Version 3.5). https://www.act.gov.au/__data/assets/pdf_file/0006/2837121/Cyber-Security-Policy.pdf.

Alberts, C. J., Behrens, S., Pethia, R. D., & Wilson, W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework, version 1.0 (CMU/SEI-99-TR-017). Carnegie Mellon University Software Engineering Institute. https://www.sei.cmu.edu/library/operationally-critical-threat-asset-and-vulnerability-evaluation-octave-framework-version-10/.

Audit Office of New South Wales. (2025). Cyber security insights 2025. https://www.audit.nsw.gov.au/our-work/reports/cyber-security-insights-2025.

Australian Computer Society. (2025). ACS backs digital productivity vision but urges action, not pause, on AI regulation [Media release]. https://www.acs.org.au/insightsandpublications/media-releases/Media-Release---ACS-backs-digital-productivity-vision-but-urges-action-on-AI-regulation.html.

Australian Cyber Security Centre. (2025a). Information security manual, Australian Government. https://www.cyber.gov.au/sites/default/files/2025-03/Information%20security%20manual%20%28March%202025%29.pdf.

Australian Cyber Security Centre. (2025b). Post-quantum cryptography figure 1 [Image]. https://www.cyber.gov.au/sites/default/files/2025-09/post-quantum-cryptography-figure-1.jpg.

Australian Government. (2017). Public Governance and Accountability Act 2013, Compilation No. 4. https://www.legislation.gov.au/C2013A00123/latest/text.

Australian Government. (2025). PSPF Annual Release 2025. Protective Security Policy Framework. https://www.protectivesecurity.gov.au/publications-library/pspf-annual-release-2025.

Australian National Audit Office. (2024). 2023–24 Performance Audit Outcomes. Australian Government. https://www.anao.gov.au/work/information/2023-24-performance-audit-outcomes

Australian National Audit Office. (2025). ANAO Annual Report 2024–25. https://www.anao.gov.au/work/annual-report/anao-annual-report-2024-25.

Australian Public Service Commission. (2025). State of the Service Report 2024–25. Australian Government. https://www.apsc.gov.au/initiatives-and-programs/workforce-information/research-analysis-and-publications/state-service/state-service-report-2024-25.

Australian Signals Directorate. (2023a). Essential Eight explained. Australian Government. https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-explained.

Australian Signals Directorate. (2023b). The Commonwealth cyber security posture in 2022: Report to Parliament. Australian Government. https://www.cyber.gov.au/sites/default/files/2023-03/The%20Commonwealth%20Cyber%20Security%20Posture%20in%202022%20-%20Report%20to%20Parliament.pdf

Australian Signals Directorate. (2023c). The Commonwealth cyber security posture in 2023: Report to Parliament. Australian Government. https://www.cyber.gov.au/sites/default/files/2023-11/Commonwealth-Cyber-Security-Posture-November-2023.pdf

Australian Signals Directorate. (2024a). The Commonwealth Cyber Security Posture in 2024. Australian Government. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2024.

Australian Signals Directorate. (2024b). Annual Cyber Threat Report 2023–2024. Australian Government. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

Australian Signals Directorate. (2025c). The Commonwealth Cyber Security Posture in 2025 Australian Government. https://www.cyber.gov.au/sites/default/fi les/2026-02/the_commonwealth_cyber_security_posture_in_2025.pdf

Australian Signals Directorate. (2025a). Planning for post-quantum cryptography. Australian Government. https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography.

Australian Signals Directorate. (2025b). Annual Cyber Threat Report 2024–2025. Australian Government. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025.

Burke, T. (2025). Cyber Security Uplift for Systems of Government Significance [Media release]. Australian Government. https://minister.homeaffairs.gov.au/TonyBurke/Pages/cyber-security-uplift-for-systems-of-government-significance.aspx.

Chhetri, M. B., Coates, R., Huang, Y., Douglas, D. M., Pathmabandu, C., Skoff, G., & Ferro, L. S. (2025). Quantum shift: How are Australian organisations navigating the quantum frontier?. CSIRO. https://www.csiro.au/en/research/technology-space/quantum-technology/quantum-readiness.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Cisco. (2025), Realizing the Value of AI: Cisco AI Readiness Index 2025. https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/2025-m10/documents/cisco-ai-readiness-index-2025-realizing-the-value-of-ai.pdf.

Critical Infrastructure Security Centre. (2024). Security of Critical Infrastructure Act 2018 (SOCI). Australian Government. https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018.

Critical Infrastructure Security Centre. (2025). The Enhanced Cyber Security Obligations Framework. Australian Government. https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf.

Department of Customer Service. (2024). NSW Cyber Security Policy 2023-2024 (Version 6.0). NSW Government. https://www.digital.nsw.gov.au/sites/default/files/2024-02/NSW-Cyber-Security-Policy-2023-2024.pdf.

Department of Finance. (n.d.). Glossary: New policy proposals (NPPs). Australian Government. https://www.finance.gov.au/about-us/glossary/pgpa/term-new-policy-proposals-npps.

Department of Home Affairs. (2022). Policy amendment – Information security. Protective Security Policy Framework. https://www.protectivesecurity.gov.au/news/policy-amendment-information-security.

Department of Home Affairs. (2023). 2023–2030 Australian Cyber Security Strategy. Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.

Department of Home Affairs. (2025). Australian Cyber Workforce Playbook (Version 10). Commonwealth of Australia. https://www.homeaffairs.gov.au/cyber-security-subsite/files/australian-cyber-workforce-playbook.pdf.

Department of Treasury and Finance. (2022). Cloud services financial guideline. Government of South Australia. https://www.treasury.sa.gov.au/__data/assets/pdf_file/0007/47383/Cloud-Services-Financial-Guideline.pdf

Digital Transformation Agency. (2025). DTA releases new guidance on Australian Government use of public generative AI tools [Media release]. Australian Government. https://www.dta.gov.au/media-releases/dta-releases-new-guidance-australian-government-use-public-generative-ai-tools.

Gartner. (2024). Gartner Forecasts IT Spending in Australia to Grow 8.7% in 2025 [Media release]. https://www.gartner.com/en/newsroom/press-releases/2024-09-11-gartner-forecasts-it-spending-in-australia-to-grow-almost-9-percent-in-2025

Justice and Community Safety Directorate. (2025a). Protective Security Framework. ACT Government. https://www.act.gov.au/__data/assets/pdf_file/0010/2567296/ACT-Protective-Security-Framework.pdf.

Justice and Community Safety Directorate. (2025b). ACT Protective Security Framework Core Practice Standards. ACT Government. https://www.act.gov.au/__data/assets/pdf_file/0009/2895309/ACT-PSF-Core-Practice-Standards.pdf.

Defence Ministers. (2024). ASDMicrosoft initiative bolsters Australia's cyber defence [Media release]. Australian Government. https://www.minister.defence.gov.au/media-releases/2024-03-18/asd-microsoft-initiative-bolsters-australias-cyber-defence

Microsoft. (2025). Microsoft Digital Defense Report 2025. https://www.microsoft.com/en-us/corporate-responsibility/cyber security/microsoft-digital-defense-report-2025/.

National Audit Office. (2025), Government cyber resilience https://www.nao.org.uk/wp-content/uploads/2025/01/government-cyber-resilience.pdf.

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST SP 800-37 Rev. 2). https://csrc.nist.gov/pubs/sp/800/37/r2/final.

Salesforce. (2025). AI Skills Gap: Demand Outpaces Readiness in Australia. Salesforce News. https://www.salesforce.com/au/news/stories/australia-morning-consult-ai-worker-readiness-report-2025/.

Singer, Y. (2025), Foundation-sec-8b: Cisco Foundation AI's First Open-Source Security Model, https://blogs.cisco.com/security/foundation-sec-cisco-foundation-ai-first-open-source-security-model

Stouffer, K., Zimmerman, T., Tang, C., Cichonski, J., Peace, M., Shad, N., Downard, W. (2019). Cyber security Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case (NIST Interagency Report 8183A Volume 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8183A-3

WPI Strategy. (2025). Update critical: Counting the cost of cyber security risks from End-Of-Life Technology on Critical National Infrastructure. https://www.wpi-strategy.com/end-of-life-tech-report

Zacks, A. (2024). Missing the Cyber security Mark With the Essential Eight. DarkReading. https://www.darkreading.com/cyber security-operations/missing-cyber security-mark-with-essential-eight.

NIIN

CISCO

UNIVERSITY OF CANBERRA