

Independent Evaluation of Cyber Hubs and Cyber Uplift

Final report

Prepared for the Minister for Finance

31 January 2023

Released by the Department of Home Affairs
under the *Freedom of Information Act 1982*

Contents

Panel Approval.....	3
Executive Summary	4
Introduction	7
Policy Context	7
Threat Landscape	8
Overview of Cyber Hubs.....	9
Independent Evaluation	11
Cyber Hubs Analysis.....	13
Defining Best Practice	13
Value for Money of Cyber Hubs	16
Increasing the Value of Cyber Hubs	17
Additional Cyber Uplift Options	20
Benefits Realisation	24
Requirements for Success for Cyber Uplift	24
Appendices	27


Panel Approval



Cathie Reid



Chris Deeble



Fergus Hanson



Nicole Ozimek



Steve McCauley

The panel would like to note that this evaluation is a point-in-time assessment, based on information gathered at the time of the review.

Executive Summary

“Cyber attacks represent a threat to our way of life. Australia has already been the target of state-sponsored cyber attacks, aimed at political parties, government departments, universities, and corporations.” An address by Prime Minister Albanese on delivering national security in a complex world

A genuine commitment is required from Government to support cyber security uplift across government. During the course of the evaluation, 4 options were identified by the panel:

Option 1: Do nothing

This option would perpetuate the continued decline in cyber resilience and maturity.

Not recommended

Option 2: The Cyber Hubs model, as proposed at December 2022

This option would provide government with three main outcomes: an added layer of perimeter defence, incident response coordination, and advisory services. However, it was discounted as it would not directly help entities with their cyber resilience which includes Essential Eight hardening, nor would it prevent a Medibank or Optus style incident from occurring.

Not recommended

Option 3: An enhanced Cyber Hubs model

The panel has found that the use of the Cyber Hubs model and its culture of collaboration, to drive coordinated cyber uplift and hardening is a viable option. However, the panel has made a number of recommendations in the Increasing the Value of Cyber Hubs section to further strengthen this model and support benefits realised.

Recommended – pending alignment to Government objectives

Option 4: Cyber uplift without Cyber Hubs

During the review it became apparent that an alternate option may exist to support targeted cyber uplift and hardening activities identified by this evaluation, without the Cyber Hubs model. This option would implement a limited subset of the cyber uplift activities outlined in Option 2, plus the off-the-shelf and collaboration capabilities outlined in Option 3, and modernise the Secure Internet Gateways. While this requires further exploration and discussion with stakeholders, the panel believes that this could be an alternate lower cost approach, as it would not require investment in the establishment of centralised hubs. However, there are challenges associated with this model, including the need to manage the delivery of uplift through robust governance.

Recommended – pending alignment to Government objectives

The panel recommends further exploration of Options 3 and 4 within a business case context to support Government to identify a preferred option.

If Government views Cyber Hubs as the preferred vehicle to uplift cyber security (options 2 or 3), including achieving the desired Essential Eight maturity, then the following are necessary to increase the value of the model:

- A clear mandate from the Prime Minister or Cabinet making onboarding to the Cyber Hubs mandatory and clarifying the program as a priority of Government

Released by the Department of Home Affairs under the Freedom of Information Act 1982

- Implementation of a tiered service offering based on an entity's baseline maturity and risk (that is based on a data-driven assessment not self-reporting)
- Clarifying and communicating roles and responsibilities within the Cyber Hubs program and considering whether there may be alternate, better suited, entities to deliver particular services through, or independent of, the 4 Hubs
- Better leveraging Australian Cyber Security Centre (ACSC) specialist capabilities, especially in relation to perimeter monitoring services such as cyber threat intelligence and system information and telemetry sharing
- The development of a whole-of-government (WofG) incident response framework that articulates roles, responsibilities, appoints a single incident response coordinator and prevents Cyber Hubs from being incentivised to prioritise protection of their own entity
- Alignment of the hubs operating model, standardising the approach across the hubs so a WofG threat picture, reporting and consistency of service can be achieved
- After the completion of Tranche 1, the panel recommends that a review be undertaken prior to any additional funding allocations to Cyber Hubs, to assess performance and priorities for next steps.

Most importantly, should Cyber Hubs be the preferred option of Government, is the need to set a long-term vision for Cyber Hubs, well beyond the current tranches. The current model centralises some cyber functions, while leaving the responsibility for IT with individual entities. This impacts the model's ability to drive meaningful cyber uplift as it is constrained to those functions which do not infringe on an agency's accountabilities.

To successfully drive cyber uplift through a centralised model, Cyber Hubs must assume responsibility for 'entities' IT.

Regardless of whether Option 3 or 4 is selected, there must be an investment in fundamental activities to get the cyber security basics correct and increase the cyber posture of government:

- Entities should be supported to share lessons learned or seek advice through the establishment of secure knowledge sharing and formal community of practice mechanisms
- A broader adoption of technical data-driven assessments, rather than self-reporting to measure cyber maturity, supported by prioritised recommendations for remedial actions
- Contractual controls should be used to enforce vendor compliance with Essential Eight requirements
- Better use of economies of scale for core or common cyber capabilities, including the establishment of a Cyber Marketplace or additional whole-of-government agreements
- Support for rapid roll-out of off-the-shelf capabilities, including Microsoft Office 365, Web Application Firewalls (WAF) and Continuous Web Application Program Interface (API) scanning and vulnerability reporting
- Recognition of the risks created by the current reliance on legacy systems and the need for a funding mechanism and transition strategy over a defined timeline
- The panel recommends that entities rapidly transition to secure cloud services environments to increase their resilience and cyber maturity
- An evaluation be undertaken into the benefits of the establishment of a whole-of-nation approach to network resilience
- Secure Internet Gateways urgently require modernisation, including a substantial policy update to cater for the fundamental shift in how government consumes IT services, including the large increase in staff operating in the cloud working remotely.

To meaningfully shift the dial in government's cyber maturity, a coordinated, programmatic approach must be taken. This will rely on clarity of vision and the development of an incremental plan towards a clearly defined, WofG North Star, such as zero trust architecture.

Major cyber security challenges for government are legacy technologies and platforms. The panel recommends conducting an independent review to assess the legacy risks and the establishment of a jointly led Digital Transformation Agency (DTA)-ACSC committee to systematically reduce the risk profile of entities and government as a whole over a defined time period.

The panel observed a consistent theme that inadequate funding of cyber security by entities has impacted cyber maturity and resilience. To address this, a commitment from Government to support appropriate prioritisation of cyber security through a fund for discrete, high-impact initiatives should be considered. In addition, the same DTA-ACSC committee should prioritise the ranking of new IT policy proposals. This would afford opportunity for consolidating smaller IT functions over time and promoting IT reuse and economies of scale.

Deconflicting the roles of the various entities in the domestic cyber security policy landscape for supporting government, including the ACSC, Attorney-General's Department (AGD), Department of Home Affairs (Home Affairs), the DTA and entities will strengthen accountabilities for delivery of various functions. Government should consider establishing a review of WofG cyber architecture to clarify these roles and responsibilities, including appropriate governance mechanisms to support strategic direction setting and accountabilities.

To align to the commitment of Government, cyber security needs to be formalised as a key organisational priority of all entities. The panel recommends the annual review of Departmental Secretary performance include the protection of public data, national security, and service delivery as a key assessable function. Government should consider holding itself to the same standards, and consequences, as the Security of Critical Infrastructure (SOCI) legislation and should demonstrate this through its own exemplar cyber security practices.

Finally, the panel notes that in an already constrained skills market, any model must be realistic, and designed in a way which considers the availability of resources to support its delivery.

Introduction

Policy context

Under the *Public Governance, Performance and Accountability Act 2013 (PGPA Act)*, accountable authorities of Commonwealth entities must establish and maintain an appropriate system of risk oversight and management for the entity, and an appropriate system of internal control for the entity. The management of cyber security risk is the responsibility of individual entities.

The key elements of the Australian Government cyber security framework are outlined in the following:

Framework/Owner	Description
Protective Security Policy Framework (PSPF)	<p>The PSPF provides direction to all government entities on secure delivery of Government business in managing protective security risks.</p> <p>The PSPF mandates 4 protective security outcomes (security governance, information, personnel, and physical security) and 16 core requirements that articulate what entities must do to achieve mandatory protective security outcomes.</p>
Information Security Manual (ISM)	<p>Outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats.</p>
Strategies to Mitigate Cyber Security Incidents	<p>A listing of prioritised mitigation strategies to help cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats.</p>
Essential Eight	<p>Provides guidance on how to implement 8 key mitigation strategies from the Strategies to Mitigate Cyber Security Incidents in a phased approach and how to self-assess the maturity of implementation.</p> <p>Since 2014, 4 of the 8 requirements have been mandatory. As of July 2022, is a core requirement of the PSPF that entities implement the Essential Eight strategies to at least Maturity Level 2.</p>

Several entities support the management of government's cyber security risk.

Cyber Stakeholder	Role/Interest
Attorney-General's Department (AGD)	Manages the Protective Security Policy Framework (PSPF) which sets out government protective security policy and supports entities to effectively implement that policy.
Australian Cyber Security Centre (ACSC)	Provides cyber security leadership and technical advice to inform the program. Provides cyber security advice and assistance to Australian governments at the federal, state, territory and local levels, business, and critical infrastructure, as well as communities and individuals.
Digital Transformation Agency (DTA)	Provides digital leadership through the application of its Investment Oversight Framework, which includes oversight of WofG programs and investment prioritisation. WofG governance and business case development coordinator for the Cyber Hubs program.
Department of Home Affairs (Home Affairs)	Home Affairs is responsible for the development and coordination of the Australian Government's cyber security policy and strategy. The department was responsible for coordinating the implementation of Australia's Cyber Security Strategy 2020. Home Affairs is also a Cyber Hub.
Cyber Hubs	Entities proposed to provide cyber services to consuming client entities under the Cyber Hubs program.
Client Entities	Consuming entities of the Cyber Hub services.

Threat landscape

Threat trends

There is an expanding range of state actors and criminal groups operating for the purpose of espionage, commercial gain, sabotage, and disinformation. The severity of cyber incidents is also increasing. For example, the ACSC's Annual Cyber Threat Report (July 2021 to June 2022), found that nearly 15 per cent of cyber incidents in 2021²² were categorised as 'Category 3', involving isolated compromise of federal government or critical infrastructure entities, up from approximately 6 per cent in the previous year. Similarly, there were 2 'Category 2' incidents, involving extensive compromise, compared to 1 such incidents in the previous year.

Commonwealth entities are attractive targets to state and criminal cyber actors as they have extensive data holdings, large customer bases, and are responsible for a range of critical functions.

Maturity and resilience of government

The Commonwealth Cyber Security Posture in 2022, released to Government in December 2022 indicated the cyber security posture across the Commonwealth requires improvement in several areas. Only 11% of entities had reached the required Maturity Level 2 for all eight of the Essential Eight mitigation strategies, which is a requirement for all Non-corporate Commonwealth Entities (NCEs).

Overview of Cyber Hubs

Concept and intent of the program

Cyber security services are largely disaggregated across the Commonwealth. While several large portfolio IT providers provide cross-portfolio IT and security services, it is normal for each Commonwealth entity to manage their cyber security services independently in line with how they manage their unique IT operating environment. This individualised approach to cyber security has led to ad hoc results and inconsistent approaches across government.

Australia's *Cyber Security Strategy 2020* introduced the Hardening Government IT (HGIT) Initiative which was intended to strengthen defences of government networks by centralising their management and operation, including considering secure hubs. Under this initiative the Cyber Hubs program has been developed to centralise cyber monitoring, detection, and response capabilities.

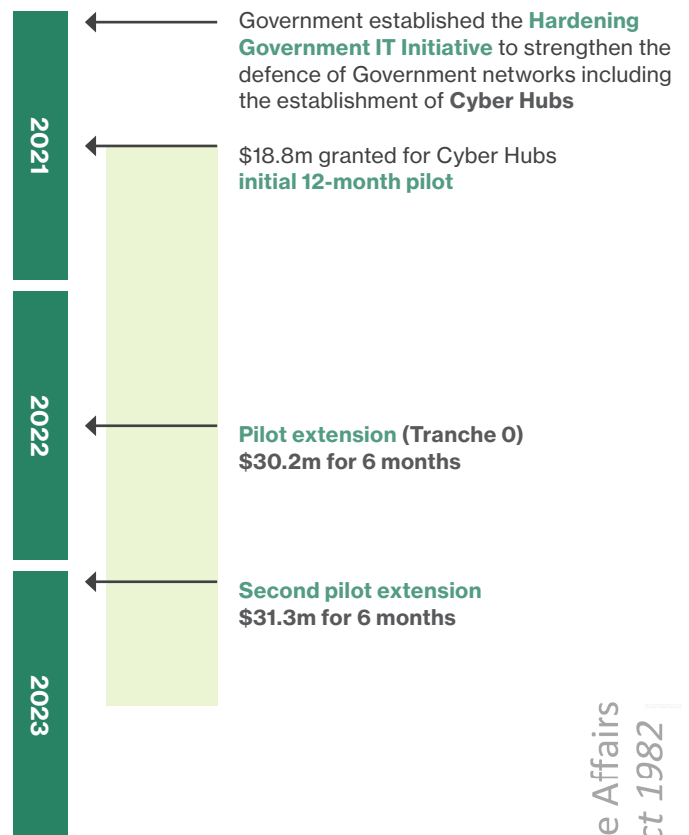
Cyber Hubs Pilot

Commencing on 1 July 2021, a pilot is currently underway to determine the feasibility of a WofG approach to monitoring, detecting, and responding to cyber threats across government.

Key deliverables of the pilot include the establishment of 4 Cyber Hubs in the Departments of Home Affairs and Defence, Services Australia, and the Australian Taxation Office, with 6 client entities to be onboarded:

- Australian Criminal Intelligence Commission (ACIC)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Civil Military Centre
- Australian Hydrographic Office
- Sport Integrity Australia
- Australian Digital Health Agency

Additional deliverables include preparing onboarding readiness assessments and transition plans for all remaining NCEs in scope of the Cyber Hubs program and conducting an independent evaluation.



Services provided by the Cyber Hubs model

The currently defined Cyber Hubs scope aims to deliver the following to 101 NCEs and 4 Corporate Commonwealth Entities:

- Perimeter monitoring (detecting attacks from known actors or vulnerabilities)
- Incident response coordination
- Sharing of threat intelligence
- System information and telemetry sharing
- Advice and assurance to support entity hardening activities

Refer to [Appendix 1](#) for further detail on the services included as part of the model and [Appendix 2](#) for Cyber Hubs client entity allocations, including identification of high priority entities.

Each Cyber Hub has developed a solution architecture to enable delivery of the above services. Importantly, these architectures are based on the development of a Maturity Level 3 environment for the hosting of these services, which is distinct from the Hub Entities' core environment and maturity.

The following key principles used to guide the development of Cyber Hubs were endorsed the Secretaries' Digital and Data Committee in August 2022.

No.	Principle
1	Provide client entities with capability uplift that is achieved by aggregating specific cyber security capabilities (such as Security Operations Centre (SOC) functions) and response to cyber threats and incidents across the Cyber Hubs program
2	Protect the most vulnerable entities from the immediate threat environment, incidents, and risks by creating a monitored perimeter. This includes providing Client Entities with advice and guidance on implementing better cyber security practices including support for 9 of the 50 controls of the Essential Eight mitigation strategies where applicable
3	Leverage quick wins and efficiencies where possible, including by aligning client allocations with WofG programs, shared services arrangements or infrastructure, and role or function where appropriate
4	Establish a broad set of five core cyber security capabilities available across government at the same cost model and pricing level. Configure these services for specific client needs so they are fit for purpose for the entity's maturity and threat environment
5	Leverage industry capabilities where appropriate through new or existing WofG sourcing arrangements and develop a cyber skilled workforce within the APS
6	Onboard client entities based on highest priority risk to achieve best uplift of cyber security across government
7	Prioritised onboarding of corporate Commonwealth entities that have a shared infrastructure with non-corporate Commonwealth entities
8	Ensure flexibility for client entities to move across Cyber Hubs
9	A client entity should be no worse off by using Cyber Hub services and meeting minimum standards

Independent evaluation

Overview

In November 2022, the Minister for Finance established an independent evaluation of Hardening Government IT and Cyber Hubs. Findings of this evaluation were to be used to inform the Cyber Hubs program and the broader refresh of the Cyber Security Strategy announced by the Minister for Cyber Security in August 2022.

Panel

The independent panel comprised:

- **Cathie Reid**, Chairperson of AuCloud, co-founder of Arc31 and a previous member of the Cyber Security Industry Advisory Committee (CSIAC)
- **Chris Deeble**, Deputy Secretary Capability Acquisition and Sustainment at Defence and a previous member of CSIAC and the Industry Advisory Panel
- **Fergus Hanson**, Director of the International Cyber Policy Centre, Australian Strategic Policy Institute
- **Nicole Ozimek**, Assistant Secretary, Cyber Security and Networks Branch at the Department of Foreign Affairs and Trade
- **Steve McCauley**, independent cyber security consultant and former Senior Executive of ACSC and IT Security leader (CISO) of numerous Federal Government entities






Scope

The purpose of the evaluation was to assess:

- better practice approaches to hardening government IT or building cyber security capability including Cyber Hubs' plans, processes, and architecture (the Cyber Hubs model)
- whether the Cyber Hubs model contributes to improving cyber security across Government by reference to:
 - if the Cyber Hubs model is viable, particularly whether cyber security services are suitable for centralisation
 - if implemented as envisioned, what benefits can government expect to see? What steps need to be taken to achieve these benefits?
 - have any unexpected negative issues been discovered? What can be done to minimise or rectify these issues?
- whether the Cyber Hubs model delivers the best value for money for the Government's investment in cyber security
- whether and how the Cyber Hubs model can best scale for 100 Non-corporate Commonwealth Entities and specified Corporate Commonwealth Entities allocated to hubs
- if the Cyber Hubs pilot has achieved agreed aims and deliverables
- other matters deemed relevant by the panel.

Methodology

The evaluation was conducted over 5 phases from November 2022 to January 2023.

Planning	Consultation	Survey	Analysis	Reporting
				
<ul style="list-style-type: none">• Established Terms of Reference• Agreed approach• Familiarisation	<ul style="list-style-type: none">• Technical interviews• Senior stakeholder engagements• Selected industry engagement	<ul style="list-style-type: none">• Hub agencies• Client entities	<ul style="list-style-type: none">• Panel meetings	<ul style="list-style-type: none">• Draft report and endorsement• Final report

The key data sources informing this report are:

- Analysis of relevant documents
- Qualitative interviews with technical representatives from cyber hub entities, pilot client entities, ACSC, industry experts, and other relevant entities
- Qualitative interviews with senior government officials
- Survey responses from both Hub entities and a selection of proposed client entities.

Cyber Hubs analysis

Defining best practice

Relevant models

While the PGPA Act, PSPF and Essential Eight set the benchmark for government requirements, there are several theoretical models which outline best practice approaches to cyber security.

The United States of America's based NIST Cyber Security Framework provides voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cyber security risk. This guidance is used much like ACSC's Information Security Manual to help organizations manage and reduce risks. It has been designed to foster risk and cyber security management communications for both internal and external organizational stakeholders.

The International Organisation for Standardization (ISO) provides the ISO 27001 standards, which are recognised as the international standard for information security. The model sets out the specification for an effective information security management system, which includes best-practice approaches to help organisations manage their information security by addressing people, processes, and technology.

The ACSC draws from these frameworks and has adapted them for Australian purposes based on the threat actors and their exploits observed. The ACSC groups its strategic guidance on how an organisation can protect systems and data from cyber threats into 4 key activities:

1. **Govern:** Identifying and managing security risks.
2. **Protect:** Implementing controls to reduce security risks.
3. **Detect:** Detecting and understanding cyber security events to identify cyber security incidents.
4. **Respond:** Responding to and recovering from cyber security incidents.

Defence-in-depth

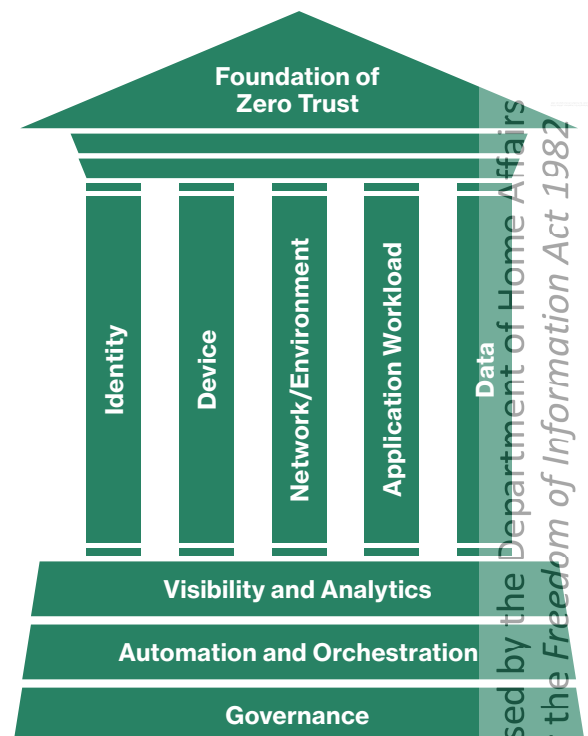
Defence-in-depth is an approach to cyber security in which a series of security mechanisms and controls are layered throughout a system to provide redundancy in the event a security control fails, or a vulnerability is exploited. The objective of this approach is to defend a system against any attack using several varying methods. If one mechanism fails, there are additional controls in place to prevent an attack.

Zero Trust Architecture

Zero Trust's primary operating principle is 'no trust without verification'. The United Kingdom's National Cyber Security Centre describes Zero Trust as:

An architectural approach where inherent trust in the network is removed, the network is assumed hostile, and each request is verified based on an access policy.

The United States of America's Government has mandated the adoption of Zero Trust Architecture requiring civilian government entities to achieve a number of milestones by September 2024.



Released by the Department of Home Affairs under the Freedom of Information Act 1982

Zero Trust is a security model in which it is assumed that no party is verified or can be trusted at any point, meaning everyone and everything must be verified continuously for access to be granted.

Applying Zero Trust Architecture can help to achieve improved cyber security outcomes.

In addition, Zero Trust Architecture can reduce the threat surface presented to malicious actors and minimise the impact of a threat actor.

There are three distinct use cases that the Australian Government should consider when thinking about future Zero Trust architecture models. These are:

1. Citizen services and critical digital functions of government
2. Third-party supply chain access to government systems
3. Government employees and the future of secure remote working

WofG and citizen identity and authentication services like myGov, myGovID and importantly the future Digital Identity capability should consider Zero Trust Architecture, and design for the required frameworks to be imbedded as part of any future updates or reviews. New cyber security services must consider this from the design and inception phases and not as an afterthought, where it will be far more costly and difficult to integrate.

International examples

A review of international approaches to cyber security identifies a variety in approaches to cyber security.

Canada

The Government of Canada adopted a single centralised shared IT services model in 2011 with the establishment of Shared Services Canada (SSC). This entity is responsible for advancing, consolidating, and providing IT services across federal government departments. A separate entity, the Canadian Centre for Cyber Security (CCCS), was established in 2018 to provide advice, guidance, and cyber security services.

New Zealand

Under New Zealand's *Intelligence and Security Act 2017*, the New Zealand Government Communications Security Bureau (GCSB) is the lead organisation for cyber security and resilience for organisations of national significance. A Government Chief Information Security Officer (GCISO) was also established in 2018.

The New Zealand GCISO is responsible for the strategic direction and prioritisation of the approach to information security and offers services to protect the Government's most sensitive information.

Under New Zealand's *Public Service Act 2020*, System Leads are mandated to lead a particular area or function across the Public Service (i.e., procurement, property, data, digital, service transformation, regions, and information security). In July 2022, the New Zealand GCISO was also appointed as the System Lead for Information Security. The Information Security Lead sets foundational information security controls for information held within IT systems that departments must follow and use performance controls to support prioritisation of digital investment to lift information security across government.

United Kingdom

In January 2022, the United Kingdom announced its £2.6 billion (roughly \$4.5 billion AUD) Government Cyber Security Strategy 2022 to 2030. The United Kingdom's investment is for government's critical functions to be "significantly hardened against cyberattacks by 2025, with all government organisations across the public sector becoming resilient to known vulnerabilities and attack methods no later than 2030.

Under the United Kingdom's National Cyber Security Strategy, the United Kingdom Government established the Government Cyber Coordination Centre (GCCC) to better coordinate cyber security efforts across its public sector. The Cyber Assessment Framework (CAF) has also been mandated as the assurance framework for government departments. However, it will be for lead government departments to adapt and apply such an approach in a way that is most appropriate for the public sector organisations in their purview.

United States of America

The United States of America's Cybersecurity and Infrastructure Security Agency (CISA) is the national coordinator for critical infrastructure security and resilience, working with federal, state, and local governments, the private sector, and international partners. CISA is the operational lead for federal cyber security, charged with protecting and defending federal civilian executive branch networks in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and federal entity Chief Information Officers and Chief Information Security Officers.

The United States of America's Federal Executive Branch employs a strategic-level coordination function under the leadership of a Federal Chief Information Officer. This model is supported by 3 funding vehicles:

- The IT Oversight and Reform Account – a central fund for Federal Government to achieve efficiency, effectiveness, and security across its IT investments, reduce cyber security risk, and implement innovative IT solutions.
- The Technology Modernization Fund – a fund to enable the Federal Government entities to access capital required to migrate off legacy platforms and technologies.
- The Federal Citizen Services Fund – a fund that enables public access and engagement with the Federal Government through an array of both public and entity-facing cross-Government shared services and programs, such as digital and data analytics programs, digital voting initiatives and the Federal Government security certification (FedRAMP) services.

In May of 2021, the President of the United States of America issued Executive Order 14028, *Improving the Nation's Cybersecurity, initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a Zero Trust Architecture by 2024.*

What good looks like

There is little debate that a layered, holistic 'defence-in-depth' approach is required to achieve effective defence against cyber threats, noting the exponential increase in the persistence and sophistication of cyberattacks against government IT.

However, there is less certainty on the value proposition and benefits of a centralised approach. It is acknowledged that a coordinated WofG approach is critical to the achievement of outcomes, but there is not clear indication that this coordination should be accompanied by the centralisation of cyber services. Nor is there consistency internationally in the approach to delivery of government cyber security outcomes.

It is the panel's view that a mature cyber posture requires a coordinated approach, aligned to a long-term vision, which is appropriately enforced, resourced, and funded.

The PSPF also highlights that while IT-related controls are critical, personnel and physical elements of cyber security, including insider threat controls are an important factor of an entity's cyber security posture.

To maintain pace with rapidly evolving threat landscape, while also considering government's legacy constraints, means that there are limited emerging security capabilities which are contextually appropriate. One such capability that the panel recommends be considered as a potential future North Star for government is a clearly defined, WofG Zero Trust Architecture.

Value for money of Cyber Hubs

The panel was provided with rough costs which indicated that it would require \$500 million over 2 years to establish the Cyber Hubs capability. Consideration of the value for money of the Cyber Hubs' program requires analysis of a longer-term cost profile, in addition to the costs associated with the initial rollout of the capability. However, the panel found the current value proposition of the model from a cyber resilience and hardening standpoint, regardless of the costs, significantly lacking.

The proposed Cyber Hubs Model is constrained to those technical and advisory services that can reasonably be provided without being responsible for an entities' IT infrastructure or business operations. It would provide 3 main outcomes to government: an added layer of perimeter detection, incident response coordination and advisory services.

The services offered within the defined scope of Tranche 1 are not substantial enough to contribute to an immediate or significant WofG cyber security uplift. Each entity remains individually responsible for implementation of the Essential Eight and other cyber controls which would prevent a cyber actor gaining access to their network or exporting data. Cyber Hubs are not able to ensure an entity acts on advisory services that they may provide. The Cyber Hubs model also will not prevent breaches, including those associated with IT misconfiguration, like the recent Optus and Medibank incidents, nor will it address insider threats. These gaps in capability need to be adequately prioritised and resourced, to ensure entities' systems are robust and resilient. Without doing so government will not be cyber resilient, despite the Cyber Hubs program.

The panel recommends further exploration of alternatives to the currently proposed Cyber Hubs model.

1. The Cyber Hubs model could deliver much more significant cyber security uplift, if it was enhanced in line with the recommendations of this evaluation, and if responsibility for IT infrastructure (servers, networks and end points) was shifted from entities to Cyber Hubs in future tranches. This transition would be complex and have significant costs but would likely result in significant cyber security improvements. There is a risk that this transition will not be able to cater to entities' individual business requirements and reduce flexibility. If the Government pursues this option, then the panel suggests clearly mapping out this vision for Cyber Hubs and client entities and providing a very strong mandate to support implementation.
2. If Government would prefer to consider an option to uplift cyber security along the lines of the currently proposed Cyber Hubs activities, without also centralising IT, there may be more cost-effective ways to achieve these outcomes without the Cyber Hubs model and the panel suggests exploring these options further.

Pilot (Tranche 0) assessment

The Pilot of the Cyber Hubs program (Tranche 0) is funded until 30 June 2023, with activities continuing until that date. As such, it was not possible for the panel to assess the success of the program in achieving its outcomes, or its value.

However, the information and data collected at the time of assessment indicated incomplete service offerings to pilot entities and dissatisfaction with the onboarding experiences and the services offered by the Cyber Hubs. Additionally, it was apparent that the client entities did not have a clear understanding of the roles and responsibilities of the program, including their reciprocal obligations, or the associated costs.

Tranche 0 was made more difficult to assess from the same baseline, as the panel identified that each of the Cyber Hubs were undertaking significantly different approaches and operating models to each other. Cyber Hubs typically choose and offered services that were the most technically achievable within their portfolio. This may reduce any benefits to WofG response, or consistency of service, particularly if an entity is required to change their hub provider.

Increasing the Value of Cyber Hubs

There are several opportunities to strengthen the currently defined Cyber Hubs model which could increase its value proposition.

Centralisation of IT

Cyber security is defined by the ACSC as “Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.” However, effective cyber security practices rely on the ability of entities to implement these guidelines (frameworks) and configure systems to mitigate risks. An entity’s cyber resilient posture relies on the underpinning IT foundations of the organisation and an in depth understanding of business operations for contextualisation. Therefore, IT and cyber security are intrinsically linked.

The Cyber Hubs model is currently constrained to those services that can be provided without interfering with entity responsibilities and accountabilities. This inhibits a hub’s ability to make necessary changes in an IT environment, preventing implementation of hardening and uplift initiatives on an entity’s behalf. Ultimately, this prevents Cyber Hubs from being responsible for the resilience of their client entities. If the current model of decentralised IT is continued indefinitely, it will impede benefits realisation of the program.

The panel acknowledges that the assuming responsibility for IT is likely to cause friction and may impact the collaborative nature of the program, but this future state must seriously be considered in a future tranche to realise the full benefits (consolidation and standardisation efficiencies) of a centralised approach.

Mandate

Should option 2 or 3 be chosen, the successful delivery of the Cyber Hubs program is dependent on a clear Government mandate to ensure uptake of the Cyber Hubs model. The model relies on the broad adoption of Cyber Hubs services from client entities to drive efficiencies and scales of economy, limited uptake will significantly reduce the model’s value proposition.

This mandate should not absolve accountable authorities of their obligations as required under the PGPA Act but should make the model compulsory for client entities. The panel believes that this mandate would be most effective if provided by the Prime Minister and/or Cabinet.

The program should be strengthened by appointing an independent accountable officer who has the support of Government to drive adherence to program outcomes. The officer should be a senior department head, who is independent of the Cyber Hubs program and potentially from a central agency.

To ensure early trust and a positive experience is provided to the client entities, it is important to ensure ahead of any mandate being established, that the Cyber Hubs program is properly defined, with clearly defined roles, operating model, responsibilities and accompanying Service Level Agreements, which all help to clarify reciprocal obligations and expectations. Consideration should also be given to clearly articulating and communicating the benefits and long-term mission of the model to client entities.

Tiered service offering

Central to increasing the benefits of the Cyber Hubs model is implementation of a tiered service offering based on entity maturity and risk. This model should focus on developing clearly defined and consistent service tiers, with accompanying Service Level Agreements, to ensure the benefits of standardisation are not lost.

Importantly, the panel recommends that this assessment not be an activity based on self-reporting, but a consistent and evidence-driven assessment which then enables a greater level of service to be offered to those entities who would benefit most.

Implementing a tiered service offering that provides the option for more services to be consumed by smaller, or less mature entities, should not equate to higher service provision with higher costs. To do so would directly disadvantage those who are being encouraged to adopt Cyber Hubs. For this reason, it is strongly recommended that all Cyber Hubs services are funded, so regardless of the entity's size, or the amount of services consumed, the costs remain neutral. A central fund should be established and administered by the DTA to ensure the intent of the Cyber Hubs program is delivered. As many services are also offered by industry and the ACSC, service costs must be proportionate and no entity is worse off for consuming them.

Cyber Hubs roles and responsibilities

Responsibilities of hub entities and client entities within the Cyber Hubs program are unclear, with feedback received regarding confusion of responsibilities and risk ownership from client entities.

The proposed hub services, being predominately assurance and perimeter based, will not negate the need for entities to still maintain their own cyber security capability. Hubs cannot be responsible for the risk to entities when they do not control the underlying IT infrastructure or business risk appetite.

There needs to be clear delineation within the program for the role of Cyber Hubs, client entities, the DTA and the ACSC in management and responsibility for the controls for mitigating cyber-attacks. Defining and appropriately communicating the delineation of roles and responsibilities should be a priority. Consideration should also be given to the suitability of these defined roles, and whether there may be alternate, better suited, entities to deliver particular services.

This should be supported by a clear definition of the scope of the program and associated services, to ensure stakeholder alignment. Stakeholder engagement, clear and concise communications and change management to ensure uptake will be just as critical to the success of the program as the technical feasibility of the model.

The definition of responsibilities for Hub entities should also include controls and associated frameworks to prevent prioritisation of their own entity.

Better leveraging ACSC specialist capabilities

ACSC monitors cyber threats targeting Australian interests and provides advice and information, including through an international network of Computer Emergency Response Teams (CERTs).

The REDSPICE initiative which was announced in the March 2022-23 Budget is a 10-year, \$9.9 billion program will triple the ASD's offensive cyber capabilities, double its persistent cyber hunt activities, and grow defensive cyber capabilities.

While the Cyber Hubs model was designed to complement ACSC's service offerings, the panel believes that the program would benefit from better leveraging ACSC specialist capabilities. This could extend to possible investment through ASD's REDSPICE program. Specific identified capabilities include:

- Cyber Threat Intelligence
- System Information and Telemetry sharing
- Additional specialist services which are required as a result of this report

ACSC has a critical advisory function and is well-placed to continue to provide assistance to Cyber Hubs and client entities. Their unique technology and tools, publications and specialist cyber security advice will provide Cyber Hubs with additional insights, best practices, threat data and intelligence, to support the provision of more tailored and targeted support to client entities. Under the REDSPICE program, ACSC will continue and evolve its existing services.

A key hardening capability acknowledged by the panel as being crucial for driving ongoing uplift across government was the ACSC's Essential Eight, Cyber Maturity Measurement Program. In support of this program, the panel suggests this specialist capability could be scaled and recommends that the ACSC and its partners, "train the trainer". This will provide additional

specialists who can undertake evidence-based (data driven) assessments and hardening outcomes for client entities. This would also free up the ACSC specialists to assist with high risk, priority uplifts and the more complicated services offerings.

The DTA should establish a WofG panel consisting of multidisciplinary specialist resources (engineers) who are subject matter experts in Microsoft Windows and Linux/Unix platforms, who additionally have experience in Essential Eight controls. This panel will assist entities which struggle to attract or retain specialist resources and allow them to draw down on and seek engineering expertise. These specialists will consume often-complex cyber security assessments, and then assist entities to uplift and rollout their recommendations. It is important to note these resources are specialist engineers (Windows Server, Active Directory, application configuration and packaging, Identity Management and so on) who also have strong experience in IT security principles, and as such, should not be confused with trying to recruit cyber security experts per se. The panel suggests that this panel could be jointly established, and then administered by the Cyber Hubs entities to leverage their scales of economy and resourcing.

Incident response

One of the key benefits of the Cyber Hubs model, as identified throughout the evaluation, is the additional incident response capabilities offered to client entities. The Cyber Hubs program will provide pre-determined resources that can be drawn on in times of need, such as a major incident. However, for these resources to be effectively used, they must be supported by a robust incident response framework, such as a federal cyber response coordination plan, that clearly articulates roles, responsibilities, and appoints a single incident response coordinator.

This framework should outline the criteria for prioritisation of effort when responding to an incident to ensure Cyber Hubs are not incentivised to prioritise protection of their own entity over their client entities.

Incident response also requires affected entities to maintain their own internal capability. Knowledge and understanding of how business systems interoperate is required, to detect, contain, eradicate and restore in the event of a system breach. Currently, entities utilise the services of ACSC in response to an incident or an industry partner that has an in-depth knowledge of their environment. ACSC should still have a strong and enduring role in tactical incident response, due to their whole of economy role, skills and partnerships.

Review post-Tranche 1

Before the completion of Tranche 1, the panel recommends that a review be undertaken prior to any additional funding allocations to Cyber Hubs, to assess performance and priorities for next steps. This review should focus on the assessment of delivery of outcomes against a defined baseline, along with articulating the expected whole-of-life cost of the program.

It will also be critical to assess whether continuing the program beyond 2 years significantly contributes to the achievement of the vision and incremental plan developed for cyber uplift across government.

Additional Cyber Uplift Options

There are several additional hardening and uplift activities which could be supported by the Cyber Hubs program or delivered through an alternate model.

Cyber partners and collaborators (option 3 or 4)

A centralised or coordinated government model, overseen by hubs or another centralised body is well positioned to provide additional value to the program by utilising their resourcing depth, leadership, and economies of scale to support the delivery of additional cyber uplift options, as recommended below, by partnering with client entities to harden and uplift their cyber security. This model would address lessons learnt from previous shared service arrangements on the pitfalls of a service delivery and service consumption model.

Through developing a culture of partnership and collaboration, rather than service delivery and consumption, Cyber Hubs or another coordinating entity will be able to assist client entities in the implementation of required and best practice cyber approaches. For example, while entities are responsible for implementation and maintenance of Essential Eight controls, Cyber Hubs can provide advice on how best to achieve the Maturity Level 2 requirement. Client entities who have achieved this milestone can also share lessons learned with their peers.

Knowledge-sharing

Government entities do not have an efficient means to share lessons learned or seek advice beyond their own personal network. Entities should be supported by establishing a secure repository with ready-to-consume resources, including security documentation created across government that could be leveraged and made applicable to their organisation and operating environment.

This repository should include establishing of whole-of-government, sector specific, communities of practice and readily available, relevant training.

Support for entity maturity assessments

Current self-reporting driven approaches to measuring cyber maturity are not driving desired uplift outcomes. An alternative approach using data-driven assessments to inform prioritised recommendations for entities to address, alongside specialist support, similar to the ACSC's Cyber Maturity Measurement Program, should be considered. This approach will support development of a clear understanding of the overall cyber maturity of government, as well as articulating the business impact level and risk of a cyber attack for an entity.

The panel notes that the skillsets required for these assessments are in demand and the feasibility of this approach may need to be evaluated.

Contractual controls

Managed Service Providers and other vendors providing IT or cyber security services to entities are a critical link in delivery of Essential Eight compliance. The evaluation identified the need for mandatory contractual controls in relevant head agreements to be considered to assure vendor compliance with mandatory cyber security requirements, including Essential Eight and PSPF controls. Consideration should also be given to assuring vendor compliance with these requirements. This is most apparent in the delivery of entities Standard Operating environment for desktops and servers where the majority of Essential Eight controls reside.

Economies of scale

Inflationary pressures, increasing licensing costs, constrained departmental operating (OPEX) budgets and a tight skills market has put some cyber services outside the range of affordability for entities. Additionally, achieving the required Maturity Level 2 for the Essential Eight comes at a significant implementation and sustainment cost for entities.

Coordination of cyber approaches and priorities across government will unlock significant economies of scale, which should be used to establish beneficial pricing for common required capabilities across government. This could be achieved through either through volume sourcing arrangements or establishment of a Cyber Marketplace.

The panel recommends that the avoidance of monopolies and a transparent market approach be a consideration for establishing any new arrangements. Any arrangements which are established should be subject to strict quality assurance and oversight to ensure effective industry partnerships.

In addition, as outlined in the DTA's Hosting Certification Framework and the ASCS's Cloud Authorisation and Hosting Framework, procurement decisions should give due consideration to data flows to ensure that nationally sensitive data is maintained by sovereign cyber security vendors and service providers ahead of multi-national providers, where possible.

Support for the rapid roll-out of off-the-shelf capabilities

Further investigation should be made into the benefits of broad adoption of supplementary, proven, off-the-shelf cyber capabilities that offer benefits to government. Priority should be given to those capabilities which support achievement of government's cyber requirements, such as Essential Eight maturity uplift. The roll out of these capabilities must be subject to strict governance to ensure adoption and, therefore, benefits realisation.

- One of the most difficult aspects of Essential Eight maturity is identifying and mitigating vulnerable systems. This issue is compounded with entities' data moving between the cloud and on-premise platforms and aging infrastructure. At most risk is internet facing systems. There are now commercial technologies that can continually test entities systems and discover unknown risks. While vulnerability scanning is within scope for Cyber Hubs, these technologies differ and are Application Programming Interface (API) specific.

The following cyber capabilities are strongly recommended by the panel and are essential to further drive cyber hardening and resilience efforts above and beyond the current scope of the Cyber Hubs program. These recommendations have taken into consideration the Optus and Medibank breaches and the cyber learnings from the Ukraine war. The panel have identified several trusted, proven technologies that could rapidly improve cyber resilience, for entities. Additionally, these capabilities provide defence-in-depth for the entities who have public internet facing applications.

These technologies recommended are, Microsoft 365, Web Application Firewalls (WAF) and Continuous Web Application Program Interface (API) scanning and vulnerability reporting.

Microsoft Office 365

The panel recommends a rapid transition of existing on-premise email and productivity suites to Microsoft Office 365 with Enterprise Security Services, as offered under the Microsoft E5 licence. Implementation should be supported by appropriate product overviews, and training to maximise its value and return of investment.

ACSC vulnerability scanning and the cyber learnings from the Ukraine war both identified immediate improvements in cyber maturity for those organisations that adopted a full cloud-based solution, rather than on-premise or hybrid approaches.

Both the ACSC and industry experts have advised that this upgrade provides a discernible overall uplift in systems and cyber resilience. If appropriately implemented and controls properly configured, entities will significantly improve their Essential Eight maturity across a number of the controls including Microsoft Office macro configuration, application controls, patching of applications, restriction of administrative privileges, multi-factor authentication, regular backups, and patching of operating systems.

Microsoft E5 licenses also offers other significant benefits such as enhanced telemetry (data about the health, email filtering and phishing controls, data loss prevention, and performance of applications) and associated reporting and analysis to inform an entity's security posture.

However, these upgraded licenses are beyond the reach of some entities, including medium to large entities, due to the headcount-based licensing model. This will need to be subsidised to avoid placing additional stress on constrained OPEX budgets. There are also migration costs, and gaps in cloud system integration expertise, which will need to be managed to support a successful transition.

Continuous API scanning and vulnerability reporting

Continuous Web API scanning and vulnerability reporting should be implemented as a priority for all entities which have public facing internet applications. This capability provides discovery and ongoing visibility of internet facing applications, including any changes in configuration, or cyber vulnerabilities that are considered high risk from a security perspective such as zero-day vulnerabilities.

Through the discovery of unknown vulnerabilities provided by this capability, and subsequent remedial actions, an entity can prevent an Optus-style breach.

An additional benefit of this capability is the ability to compare reports, which can be used to check for human errors during periods of major change, including major IT releases. For example, a pre- and post-release scan and report of an entity's APIs after a significant change cycle, could identify a significant vulnerability.

This capability is seen to complement, not duplicate, the Cyber Hygiene Improvement Program (CHIPs) run by ACSC. CHIPs tracks and monitors the cyber security posture of Australian, state, territory and local government entities' internet-facing assets. CHIPs also conducts rapid operational taskings when potential cyber threats emerge, such as newly disclosed vulnerabilities.

Web Application Firewalls

Web Application Firewalls (WAFs) protect web applications by filtering and monitoring incoming traffic. This includes identifying malformed or malicious web requests and blocking them. This capability forms another layer in the defence-in-depth attack mitigation and will help harden systems against common malicious activities.

WAFs complement, but are not dependent on, the Continuous Web API scanning capability by providing a filter that recognises attack patterns and prevents access to the target application or its API. The panel considers all entities should implement WAFs.

Network resilience

As part of the consideration of supplementary capabilities, the panel considered the benefit in establishing a Government National Network. The proposal would consolidate network traffic for government onto a dedicated network to provide protection and options for government to respond to a major cyber attack.

The panel notes that there is limited benefit to a solution solely focused on the federal government level, due to the interdependencies with critical infrastructure and other levels of government in the provision of services. However, the panel is supportive of an evaluation of the establishment of a whole-of-nation approach to network resilience, with the aim of maintaining services of government during a major cyber incident for critical infrastructure as well as government. This evaluation should consider benefits to government, industry, and citizens but notes that it should be considered within the broader cyber incremental plan.

It is critical that the potential establishment of any network does not adversely affect competition within the sector.

Transition to cloud

The panel recommends that entities rapidly transition their backend application and server environments to a secure cloud services environment. Similar to Microsoft Office 365, this shift would uplift the cyber maturity and resilience of most entities by addressing several of the Essential Eight controls (if appropriately configured), including regular backups, patching of operating systems, and patching of some applications application controls, multi-factor authentication and restriction of administrative privileges. Additionally, the transition will achieve many ISM controls that are required for an IRAP certified Protected platform-as-a-service environment.

Cyber lessons learnt thus far from the Ukraine war indicated that government entities that shifted to cloud platforms were far more resilient to threat actors.

Shifting to cloud services will deliver security benefits but not immediate cost advantages. During transition, costs often peak due to the requirement to maintain both premise and cloud services during migration.

Due to cloud services predominately being an OPEX expense, entity's IT budgets will need to account for the pivot from their current focus on capital expenditure (CAPEX) for purchase and maintenance of fixed assets.

While the Department of Finance governs a process for funds to be reclassified from CAPEX to OPEX, it is clear that the shift is still perceived as a significant issue to navigate by many entities, and it is often easier to default to continuation of CAPEX processes that officers are familiar with.

The removal of these perceived barriers are critical to escalate cloud migration and achieve the accompanying uplift in cyber resilience.

Secure Internet Gateways

Since 2011, a policy has been in place to consolidate gateway services for Commonwealth entities under a lead agency gateway model. There are currently 6 lead agency gateways, which predominantly use commercial partners to give effect to the gateway requirements.

Secure Internet Gateways (SIGs) provide government entities with a range of cyber security and network communication capabilities. The cyber capabilities offered are not dissimilar to those proposed by the Cyber Hubs model. However, they have stagnated over the years due to a lack of investment, compliance oversight, and policy updates based on the ongoing expectation of the Cyber Hubs program.

There is a requirement for their modernisation, including a substantial policy update to cater for the fundamental shift in how government consumes IT services, and the large uptake in staff operating in the cloud or working remotely.

As they currently stand, SIGs lack the required capabilities and incentives to cater for a contemporary government workforce that has a larger proportion of remote workers and is subsequently operating more from edge networks (as opposed to a centralised model). Technologies are available for consumption today that have bridged these gaps, (some are already servicing government), such as Software as a Service (SaaS) technologies that provide secure connections between users and their applications, regardless of device, location, or network and native cloud hosting environment.

Other gaps include the need for more contemporary service offering that facilitates telemetry sharing and data parsing for the consumption and analysis by the ACSC.

Many of the defence-in-depth recommendations made, would provide supplementary cyber resilience to both the Cyber Hubs and SIG's perimeter defences. This includes log ingestion into Security Operation Centre (SOC) / Security Incident and Event Monitoring (SIEM) offerings and 24x7 or around the clock monitoring for entities.

Cyber Hubs perimeter monitoring is prefaced in receiving a feed from a SIG. There have been some delays in the rollout of Cyber Hub service offerings and onboarding entities, which relate to contractual issues with Secure Internet Gateways Managed service providers and the associated contract which will incur financial penalty. These also require updating as part of the SIG policy refresh.

Benefits realisation

Requirements for success for cyber uplift

A clear North Star

In a speech to the Lowy Institute in March 2022, the Prime Minister articulated his vision for national security, with a priority on *better and smarter cyber security*.

“Keeping Australians safe means planning for global shocks – be it conflict, pandemic, financial collapse, or environmental disaster. And investing in the country’s capacity to adapt to crisis, building the resilience and resolve to ensure we can come through challenging times together.

“Our security agencies are very good at what they do in this space, but true national cyber resilience is a whole-of-nation endeavour.”

Universal cyber uplift across all government entities requires a coordinated approach and is contingent on stakeholder buy-in and effective monitoring of progress against defined outcomes. There must be clarity on the vision for cyber security, such as the transition to a Zero Trust Architecture approach.

To support the achievement of this vision, an incremental plan must be developed, incorporating defined responsibilities for delivery and oversight. Ongoing investment and engagement in uplift activities is dependent on the associated complexity being described in succinct and digestible terms. Focus should be given to articulating the discrete cyber uplift requirements of government entities and appropriate governance, responsibilities, and accountabilities for the program of work.

The panel acknowledges that there are multiple streams of uplift to be incorporated into this plan, including Essential Eight uplift, implementation of core or common capabilities, legacy system transition and broader PSPF requirements. However, consideration must be given to the individual business risk and impact level of an attack on an entity as a means of prioritising uplift activities.

Legacy review

Legacy technologies are severely impacting Australia’s cyber security resilience as they are difficult, or impossible to secure due to unsupported software or operating systems, that can no longer be patched.

In the ACSC’s *Annual Cyber Threat Report (July 2021 to June 2022)*, it was identified that malicious actors routinely scan for vulnerabilities years after they are initially disclosed, targeting networks which are running legacy software or have failed to patch. A 28 April 2022 Joint Five-Eyes Advisory observed that 6 of the top 15 Routinely Exploited Vulnerabilities in 2021 were first disclosed in 2020 or earlier.

There is a need for an independent review to assess the legacy risks of entities and determine priorities for action to systematically reduce the risk profile of entities, and government as a whole, beyond current investment prioritisation activities conducted by the DTA. This must be a genuine long-term plan with immediate actions identified to mitigate and reduce the significant risks associated with legacy technologies. This transition will come at a significant cost but cannot be delayed or avoided without continuing government’s current intolerable risk profile.

It is important to note that ongoing avoidance to address the legacy system upgrades or migrations will continue to have a compounding monetary impact, as the challenges become increasingly more complex and expensive to deal with.

The panel recommends establishing a joint DTA-ACSC committee to define a comprehensive WofG plan and oversee the required transition activities with consideration to factors such as service delivery and national security.

Once developed, this should be incorporated into the incremental plan for cyber uplift. A further benefit when refreshing infrastructure and monitoring for end-of-life systems, will be the opportunities identified for IT reuse and consolidation, where it makes sense.

Funding

“Threat actors across the world continue to find innovative ways to deploy online attacks, as a result too many Australians have felt the impacts of cybercrime. That is why the Government is committed to reinforcing Australia’s cyber security as a national priority.”

- Deputy Prime Minister and Minister for Defence, the Hon Richard Marles MP

The panel observed a consistent theme over the course of the evaluation that inadequate funding of cyber security by entities has impacted capacity and capability to meet minimum cyber security requirements. At the same time, these requirements have evolved over time necessitating additional effort and resourcing to maintain cyber maturity.

Several factors, including the rapid uptake and shift to cloud computing, have heavily impacted available departmental OPEX budgets. In addition, inflationary pressures have resulted in rising software and hardware costs, and an extremely competitive contractor market, combined with excessive delays exacerbated from COVID supply chain issues has put significant pressure on departmental IT budgets.

While this increase has occurred, entities have prioritised competing priorities over cyber security and their existing IT budgets, are getting less for their dollar, which has negatively impacted cyber security outcomes.

To address this, a genuine commitment is required from Government to support appropriate prioritisation in cyber security investment.

Cost recovery or charging for Cyber Hubs

If Cyber Hubs proceed, the implementation of cost recovery or charging models after the first 2 years may undermine uplift efforts by continuing to limit available funding. However, it is also recognised that there may be savings through the implementation of broader scales of economy in procurement, and quick wins that will deliver immediate productivity gains that avoid unnecessary duplication. It is the panel’s view that efficiencies should be reinvested into further cyber initiatives to support uplift.

Cyber security fund

Additionally, a cyber security fund should be considered for discrete, high-impact initiatives with appropriate governance to be implemented to ensure funds are allocated to those activities which align to the incremental plan and will represent the best value for money.

This would enable more dynamic and agile funding arrangements to be implemented for lower-cost initiatives that would achieve uplift outcomes. This would comply with Budget rules for defined cyber uplift activities that may otherwise inhibit bids for cyber uplift by entities, particularly where offsets are not available, or the measure has a relatively low cost and may be required to be absorbed.

A fund could also drive transparency of cyber capability maturity, which is currently opaque across entities, for instance as a precondition to making a bid for funding.

A fund would need appropriate governance and Ministerial oversight. The panel's view is that the DTA should administer such a fund with support and involvement of the ACSC, AGD and central entities in decision-making. Such a fund could be overseen by the Secretaries' Digital and Data Committee under the Minister for Finance and Minister for Cyber Security.

The priority measures recommended in this evaluation report should be the starting point for a fund, including Essential Eight uplift.

Clarity of WofG cyber roles

There is a requirement across government to deconflict the roles of the various entities in the cyber security policy landscape, including the ACSC, AGD, Home Affairs, the DTA and entities. There may also be a need for a refresh of the machinery of government to support a more streamlined cyber architecture. This would provide clarity in roles and responsibilities will strengthen accountabilities for delivery of various functions.

By articulating a clearly mandated, holistic strategy which is underpinned by an incremental plan, and unambiguous accountabilities, roles and responsibilities, government will be able to drive effective stakeholder engagement and alignment.

Accountability for cyber uplift

Cyber security uplift is not being achieved at the pace required to address the worsening threat environment. Despite articulating requirements under the PSPF and Essential Eight, these obligations are not being adhered to by government entities, due to a range of factors including monetary, resourcing or competing pressures with limited consequences. With the cyber skills shortage accountable authorities may also not have the requisite expertise within their entity to appropriately advise them on the risks they are carrying.

This does not align to the approach taken to ensure uplift of industry, with clarity of legislative and regulatory accountabilities and associated consequences of non-compliance under the SOCI legislation.

Cyber security needs to be formalised as a key organisational priority of all government entities. A consistent theme throughout the evaluation was the role of the accountable authority in the management of their entity's cyber security risks. For government to be cyber resilient, the accountable authority must prioritise cyber security and source, and allocate commensurate funding to their risks to protect their information and systems.

Under section 61A of the *Public Service Act 1999*, an annual review of the performance of each Departmental Secretary must be undertaken in accordance with a framework established by the Secretary of the Department of Prime Minister and Cabinet and the Australian Public Service Commissioner. The panel recommends expansion of the key assessable functions to include the protection of public data, national security, and service delivery.

This could be supported by providing granularity of appropriate cyber security obligations as Key Performance Indicators (KPIs), to be reported through Secretary Scorecards. These KPIs should consider relevant cyber security metrics, for example driving improvements in Essential Eight maturity.

Resourcing

The panel acknowledges that several of the recommendations made in this report will require additional resources to deliver uplifted capabilities. In an already constrained skills market, any model must be realistic, and designed in a way which considers the availability of resources to support its delivery.

Appendices

Appendix 1: Tranche 1 Scope of services with program governance and enablers

	Cyber incident response coordination			Cyber Threat Intelligence (CTI)		
	Services	Incident response advice and coordination	Incident detection and notification (high priority onboarded entities)	Incident detection and notification (all client entities)	CTI consumption	CTI feedback
Vulnerability assessments (high priority onboarded entities)		Vulnerability assessments (all client entities)	Lead incident response	CTI sharing (non-contextual reports)	CTI sharing (targeted entity reports)	Threat hunting
System information and telemetry sharing			Endpoint hardening advice and assurance		SIEM and SOC	
System information and telemetry (through auPDNS &HBS)		System information and telemetry sharing (through more protocols)	Advice conducting Essential Eight maturity assessments	Endpoint security enhancement	Log ingestion (high priority onboarded entities)	Log ingestions (all client entities)
			Vulnerability management		Log monitoring and analysis (high priority onboarded entities)	Log monitoring and analysis (all client entities)
Governance	Program Delivery			Operational		
	Operational, Governance and Coordination Working Group	Funding and Charging Working Group	Cyber Hubs Executive Group (Band 2)	Client Entity CISO	Cyber Hubs Senior Responsible Officers	CCSOC, Secretaries and Ministers
	Program Management, Risk and Security					
	Privacy and Legal Issues Working Group	Cyber Hubs Delivery Team (Band 1)	Secretaries Board and Secretaries Digital and Data Committee	Comms/Change management, stakeholder engagement	Architectural solutions, operational plans, transition plans	Risk/issue management, quality assurance and evaluation
Enablers	Preparatory Services			Implementation	Strategic	
	Onboarding readiness activities (PIA and MOU's)	Gateway services for client entities	Assist to implement ACSC "quick wins" e.g. DMARC, TLS and auPDNS	Project management, data and reporting	Home Affairs coordinated incident Reponse Framework	Workforce planning
	Establish bi-directional CTI consumption via CTIS platform	Operational Governance for cyber incident management	Improve event log standardss	Program operations and Governance	PSPF, Essential 8, Cyber Security Strategy	Whole of Government Cyber Security Uplift Roadmap

Key

Commence Tranche 0

Tranche 1 and Future

Future Tranche only