Australian Government
Defence

DEFENCE CYBER SECURITY STRATEGY

ISBN: XXX

CONTENTS

This page intentionally left blank.

FOREWORD

Future conflict will involve sophisticated cyber warfare. Nations across the globe have recognised the strategic value and asymmetric advantage of investment in offensive cyber capabilities. They continue to evolve and advance their capabilities, strategies and tactics, contributing to a deteriorating strategic environment. As you read this Strategy, adversaries and cyber criminals are probing Defence's networks for vulnerabilities to exploit. They are seeking insights into Defence capabilities, platforms, and personnel. They are seeking to steal data, slow Defence's work, impact operations and identify gaps to exploit in the future.

Malicious cyber activity now represents one of Defence's most critical risks. Our cyber security is therefore now one of our most critical tools to defend our people, capabilities, and ultimately, our nation. Defence's response must be deliberate and decisive to address the worsening cyber threat environment. The *Defence Cyber Security Strategy* will position Defence to defend Australia and advance our security and prosperity.

This Strategy details how Defence will combat cyber threats and ensure its capabilities are secure against attacks from adversaries. This will require a concerted and coordinated effort across the entire Defence ecosystem, from Australian Defence Force and Australian Public Service personnel to Defence's industry partners and supply chain. Each part of this ecosystem contributes to, and has a role to play in ensuring, the cyber security of Defence, and our nation.

This Strategy presents the path to a cyber resilient Defence and the principles to maintain a strong cyber security posture in a shifting strategic environment. It is essential that this be accompanied by strong leadership, resolve and a willingness to transform from across the Defence ecosystem. Together we can ensure a strong Defence, and the future security and prosperity of Australia.

In response to our rapidly changing strategic circumstances, the Government has committed to a Defence Strategic Review that will examine force structure, force posture and preparedness, and investment prioritisation, to ensure Defence has the right capabilities to meet our growing strategic needs. In an environment characterised in particular by increased cyber threats, the Defence Strategic Review will provide a comprehensive assessment so Defence remains positioned to meet growing regional and global challenges.

Consequently, the implementation of the *Defence Cyber Security Strategy* will be responsive to and informed by the outcomes of the Defence Strategic Review so that it maintains strong strategic alignment and is able to meet Defence's future needs.

The Hon Matt Thistlethwaite MP

Assistant Minister for Defence

Assistant Minister for Veterans' Affairs

31 August 2022

This page intentionally left blank.

EXECUTIVE SUMMARY

Defence must continue to improve its cyber security if it is to defend against constant malicious cyber activity and succeed in future conflicts. This is necessary for the continued fulfilment of Defence's mission, and the continued delivery of critical functions upon which our national interests rely, and all Australians expect.

The Strategy will shape the Defence portfolio's cyber security for the next ten years. It establishes the guiding principles and strategic objectives to enhance Defence's cyber security capabilities in line with the shifting threat environment. The Strategy also establishes four priority action areas that outline objectives to be achieved over the next three years. This will set the necessary foundations for Defence to be a cyber security exemplar now, and into the future, as cyber threats evolve.

This Strategy will ensure Defence can continue to transform, adapt and evolve securely. It will support Defence's ability to Shape, Deter and Respond: shaping its cyber security environment through uplift, standards setting and strengthened partnerships; informing its deterrence activities through improved visibility of adversaries' activity; and refining its ability to respond by enhancing its cyber security posture and limiting adversaries' ability to conduct malicious cyber activity against Defence.

The nature of cyberspace means that every capability, every individual and every industry partner represents a target and opportunity for adversaries. This Strategy recognises that the unprecedented threat environment Defence faces extends across its industry partners. The need for industry partners to establish and maintain strong cyber defences has never been more critical. This Strategy can only be achieved through a concerted effort across Defence's entire ecosystem, working together to strengthen our collective cyber security and defend Australia.

STRATEGIC CONTEXT

The *2020 Defence Strategic Update* detailed the deteriorating nature of Australia's strategic environment and the contributing role of cyber capabilities. Cyber threats are increasing in sophistication and scale. Cyber has emerged as a recognised warfighting domain and cyber warfare will be a critical component of future conflict.

Defence operates in complex and contested terrains that present significant and unique challenges for its cyber security capabilities. The requirement for cyber security is more critical than ever, and the scope extends well beyond Defence's immediate networks and warfighting capabilities. Defence industry and supply chains, related critical infrastructure, and Australia's research and development sector are a significant target for adversaries. Defence relies on the security of more systems and capabilities than ever before, and in an increasingly hostile cyber threat environment. This calls for a hand-in-hand approach with industry to uplift the security of the entire Defence ecosystem.

The threat does not stop at the high-end capabilities of Defence and industry. Individuals within the Defence ecosystem, both Defence personnel and industry contractors, are being targeted as an indirect entry point to compromise Defence's networks and capabilities. Adversaries continue to deploy unrelenting and increasingly sophisticated malicious cyber campaigns at scale to compromise individuals, collect their data, and infiltrate, disrupt and deny Defence capabilities. Everyone connected to the Defence ecosystem must play their part.

Poor cyber security has the potential to severely impact the utility of Defence's ships, aircraft, weapons systems and supporting capabilities, such as bases and critical infrastructure. As a likely pre-cursor to and critical element of future conflict, Defence's cyber security posture will likely be a determining factor of Australia's success or defeat.

Ultimately, the fulfilment of Defence's mission is dependent on cyber security.

> *Cyber-attacks can directly compromise military capability and operations. Cyber-enabled activities can also drive disinformation and destabilising interference in economies, political and social systems and infrastructure.*
>
> *- 2020 Defence Strategic Update p. 13*

STRATEGIC VISION

The Strategic Vision provides an enduring direction for Defence's cyber security over the next ten years. Delivering on this Vision is critical to ensure Defence has the cyber security capabilities, structures and partnerships necessary to deliver on its core mission, and combat current and future threats in an ever-evolving strategic environment.

The Strategic Vision is:

MISSION-FOCUSSED, THREAT-CENTRIC AND **CONTEMPORARY** DEFENCE ENTERPRISE CYBER SECURITY, ENABLED BY **BEST-PRACTICE** AND **STRONG PARTNERSHIPS**

PRINCIPLES

The Strategic Vision highlights guiding Principles that must drive all of Defence's future cyber security activities over the next ten years. These Principles provide a guiding framework for all Defence personnel, and the enterprise at large, on how to focus and align cyber security efforts, capabilities and resources at every level and across every function.

The Principles are:

MISSION-FOCUSSED

Defence will align its cyber security efforts in support of its core mission and business operations.

STRATEGIC OBJECTIVES

- Defence allocates and prioritises cyber security resources to those areas that present the greatest risk to the mission.
- Defence's cyber security is a key enabler of its mission and operations. Defence is able to deploy secure technologies to achieve mission objectives and protect Australia.

THREAT-CENTRIC

Defence's cyber security capabilities will be commensurate with the threat environment and capable of quickly adapting to match the evolving threat landscape.

STRATEGIC OBJECTIVES

- Defence is prepared for future threats and constantly adapts to remain one step ahead of adversaries.
- Defence has agile cyber security capabilities that can be rapidly deployed against cyber threats, and its cyber domain can quickly adapt to remain cyber secure.

CONTEMPORARY

Defence will continue to modernise, enhance and optimise its cyber security capabilities.

— STRATEGIC OBJECTIVES

- Defence's cyber security capabilities, including personnel and technologies, are cutting edge and achieve force multiplication effects.
- Defence's technology investments are informed by intelligence and modernised to enable cyber security outcomes.

BEST-PRACTICE

Defence will refine its cyber security foundations to align with leading standards.

— STRATEGIC OBJECTIVES

- Defence's governance structures, capability processes and people management policies enable its networks, systems and warfighting capabilities to be secure and meet leading cyber security standards.
- Defence adopts leading cyber security standards that strengthen its cyber security posture.

STRONG PARTNERSHIPS

Defence will strengthen cyber security partnerships with government, industry, academia and international partners to enhance situational awareness, resourcing, and cyber security capabilities.

— STRATEGIC OBJECTIVES

- Defence has access to secure supply chains and vendors who contribute to a cyber secure Defence ecosystem.
- Defence has strategic partnerships leveraging the best of Australian and allied expertise and capabilities, particularly in times of crisis.
- Defence's partnerships are mutually beneficial, provide greater cyber threat awareness and contribute to a whole-of-economy cyber security uplift.

THE PLAN

The Strategic Vision and Principles will be initially realised across four priority action areas. These action areas will further enhance Defence's cyber security foundations over the coming three years. Following this initial three year period, the Strategic Vision and Principles will underpin continued cyber security activities for the life of the Strategy.

CYBER SECURITY GOVERNANCE

Reforming Defence's *cyber security governance* to enable and empower its cyber security apparatus as a potent warfighting capability.

CAPABILITY MANAGEMENT

A renewed approach to *capability management* that is informed by and responsive to cyber threats, delivers effective risk engagement and prioritisation of finite resources, and is supported by strategic partnerships.

PEOPLE

An innovative approach to *people*, recognising the level of competition for cyber security talent, and that a cyber secure culture must be a part of the entire Defence ecosystem.

FUTURE READY

A revitalised focus on researching, developing and investing in future cyber security capabilities to stay ahead of adversaries and ensure Defence is *future ready*.

CYBER SECURITY GOVERNANCE

Strong cyber security governance is critical to ensuring the effectiveness of Defence's people and capabilities. While Defence has a strong foundation, rapid changes in technology and the strategic environment necessitate a refresh. Defence's cyber security governance frameworks and policies must enable Defence to effectively combat cyber threats, succeed in its warfighting mission and ultimately defend the nation.

An optimised cyber security operating model is key to achieving these effects. Defence's cyber security operating model must support a coordinated and consistent approach to cyber security, delivering further operational efficiencies as Defence's cyber security capabilities continue to be asked to do more in an increasingly complex environment. The operating model will need to account for the increasingly cross-cutting nature of cyberspace, while ensuring that appropriate mechanisms are in place to enhance Defence's cyber security risk management and investment decisions. It should further enable strategic partnerships with industry, acknowledging industry partners' critical role in Defence's overall cyber security posture. It must also enable deeper cyber security partnerships and interoperability with our allies.

The operating model refresh will include a strengthened and empowered central cyber security entity that is enabled to manage Defence's collective cyber security risks, provide clear, consistent and rapid guidance, respond to evolving cyber threats with speed and agility, and drive a coordinated approach to cyber security. This will be supported by the delineation of clear cyber security roles, responsibilities and authorities across the enterprise, and a recalibration of Defence's cyber security workforce to ensure efforts continue to be aligned to mission priorities. This will take into consideration the growing role of industry partners in strengthening Defence's cyber security.

Defence will continue to adopt best-practice standards and review its cyber security policies to ensure frameworks support a consistent and fit for purpose approach to cyber security. These policies must support wide adoption and application across the enterprise, and with industry partners. Critically, these policies must enable Defence's cyber security capabilities in times of conflict and cyber warfare, reinforce a reformed operating model and ensure capabilities continue to be cyber secure in response to rapidly changing threats.

OBJECTIVES

The objectives of the initial *cyber security governance* actions are to:

- implement an optimised cyber security operating model that enables Defence's cyber security capabilities and its warfighting mission;
- maximise operational efficiencies and return on investment through strengthened and more centralised cyber security governance;
- clearly define cyber security roles, responsibilities, accountabilities and authorities across Defence;
- adopt clear, practical and consistent cyber security policies that support the cyber resilience of Defence capabilities during all phases of operations, including conflict; and
- set a cyber security baseline through the adoption of recognised and Defence-relevant cyber security standards.

CAPABILITY MANAGEMENT

All of Defence's capabilities operate to some extent in and through cyberspace. This poses a challenge given Defence's diverse and widely dispersed array of networks and warfighting capabilities. Coupled with a worsening cyber threat environment, a shift in how Defence manages the cyber security of its capabilities, and how it leverages its partnerships with industry is required.

Defence will undertake a range of activities to improve the foundational aspects of procurement arrangements and to strengthen strategic partnerships with industry. Given the fast paced cyber threat environment, Defence will work with industry to streamline cyber security capability acquisition pathways and processes. This work will include exploring potential processes and partnership arrangements necessary to enable the rapid acquisition of Australian and allied expertise in the event of a crisis.

Defence will also improve how it manages the cyber security of capabilities, ensuring cyber resilience and battle readiness. This will include elevating cyber security as a key consideration in the acquisition, sustainment and decommissioning of capabilities, and the improvement of risk management processes. Acknowledging industry's key role in the cyber security of Defence capabilities, Defence will continue to strengthen the *Defence Industry Security Program* to both improve cyber security outcomes, and streamline the program for industry. These activities will ensure a coordinated approach from Defence and industry to uplift cyber security across the Defence ecosystem.

To ensure the best use of its finite resources, Defence will reform its risk analysis mechanisms to enhance capability prioritisation. This activity will focus on ensuring Defence capabilities are continually directed towards critical risks. This will also support a reduction in the number of legacy systems that create cyber risk for Defence, while enabling Defence to effectively prioritise, maintain and secure those assets unable to be replaced or decommissioned.

OBJECTIVES

The objectives of the initial *capability management* actions are to:

- enable the rapid and agile acquisition of cyber security capabilities and expertise;
- ensure cyber security requirements are adequately considered in the design and acquisition of new capabilities, and improve cyber security across all phases of the lifecycle;
- signal Defence's expected cyber security standards to industry and its supply chain, and deliver an uplift across Defence's ecosystem;
- effectively manage cyber security across Defence's diverse range of capabilities; and
- ensure Defence's finite resources and capabilities are focussed on critical risks and mission priorities.

PEOPLE

At the core of Defence's cyber security capability is its people. Unlike other warfighting domains, everyone has a direct role in the security of the cyber domain. Everyone that interacts with the Defence environment and supply chain presents a potential target and opportunity for adversaries. One action, by one user, could expose critical information or create an entry point for an adversary. An adversary could take advantage of this to compromise aircraft, ships, personnel, weapon systems and critical support functions, and threaten Defence's ability to succeed across all warfighting domains. The significance of these risks necessitates a recalibration in how Defence approaches cyber security across the workforce.

Defence's approach to cyber workforce management needs to meet current and future needs. Traditional workforce management techniques must be adapted, particularly given the competition for cyber security talent.

Defence will explore new strategic partnership arrangements with industry and allies that allow Defence to tap into broader talent pools in times of crisis. Defence will take advantage of the unique elements of its cyber security operating environment to attract and retain talent. Innovative approaches to talent management and professional development will be explored to strengthen the workforce pipeline and develop future leaders. These activities will align with and contribute to the *Cyber Security National Workforce Growth Program*, a joint initiative undertaken by Defence, the Department of Home Affairs, industry and academia.

Every individual that interacts with Defence networks and those within its supply chain must also understand that they are a target and are connected to the warfighting domain. Defence will undertake a revitalised cyber security cultural change program to ensure that every individual understands that their behaviours at work and when remotely connected, along with their personal digital footprint, can impact Defence's cyber security and create risks for the individual, and their family and friends. The cultural change program will be supported by a strong Defence-wide cyber security training program designed to equip personnel with the skills they need to be cyber secure. Defence's senior leadership will continue to play a critical role, reinforcing a cyber secure culture across the enterprise and promoting the direct role that every individual plays in Defence's overall cyber security.

OBJECTIVES

The objectives of the initial *people* actions are to:

- define and meet Defence's current and future cyber security workforce requirements;
- build awareness of cyber security threats and individual accountabilities, and uplift cyber security capability across the Defence workforce;
- increase the ability of decision-makers to incorporate cyber risks into their risk management practices; and
- explore innovative approaches to talent management and professional development to attract and retain personnel, and build future cyber leaders.

FUTURE READY

The strategic environment is constantly evolving, particularly in relation to cyberspace. Sophisticated cyber actors are rapidly adapting their tactics and developing new capabilities and Defence must keep pace to ensure it can effectively engage in future warfare and fulfil its mission to defend Australia.

Defence has the challenge of implementing and securing a significant and diverse array of new and sophisticated business systems and warfighting capabilities. The compromise of any one system or capability could result in strategic advantage for an adversary.

To match the rapidly evolving cyber threat environment, Defence must be able to quickly adapt to, and employ emerging security approaches. Innovative approaches to security, not only at the technical level, but those that apply to governance models, policies and workforce practices must be considered to enable Defence to protect critical systems and defend against malicious activity. To achieve this, Defence will identify immediate cyber security investments necessary to ensure it is at the cutting edge of cyber security. These investments will seek to not only enhance Defence's cyber resilience, but ensure interoperability with existing capabilities while minimising capability duplication across the Defence portfolio. Defence will continue to collaborate with allies to inform investments, align capabilities and build our collective cyber security.

While maintaining and strengthening its current systems and capabilities, Defence must have one foot firmly planted in the future to ensure it maintains technological pace with its adversaries. Based on threat intelligence, Defence will strengthen its longer term research and development programs to ensure it has the strategic cyber security capabilities necessary to combat future threats. Research and development will be targeted at those capabilities most likely to provide force multiplication effects, including automation and artificial intelligence, in preparation for a more severe cyber threat environment.

However, research and development alone is not sufficient. Defence must ensure it is able to industrialise and operationalise these research outcomes from concept to capability. Ideally, this needs to be achieved in a sovereign ecosystem to deliver strategic advantage and grow the domestic cyber security market. Defence cannot achieve this in isolation, and will leverage strategic partnerships with industry, small to medium enterprises, academia, think tanks, allies and international partners to develop a capability realisation pathway for the future.

OBJECTIVES

The objectives of the initial *future ready* actions are to:

- identify and address existing and future gaps in Defence's cyber security capability;
- amplify the capability of Defence's cyber security workforce through strategic investment in new and emerging technologies;
- continue to align investment in new cyber security capabilities, and research and development activities with allies to ensure Defence's investment in cyber security achieves maximum impact; and
- leverage strategic partnerships with industry, small to medium enterprises, academia, think tanks and international partners to fully harness research and development opportunities.

WHERE TO FROM HERE?

This Strategy is designed to deliver on the objectives of the *Defence Transformation Strategy*. It will contribute to a high-performing One Defence enterprise with the ability to continuously improve and adapt to changing strategic circumstances.

A robust cyber security apparatus will be a key determinant in the success of Defence's mission, now and into the future. Accordingly, this Strategy provides a flexible, principles-based approach to ensure Defence is well-positioned to meet future cyber security challenges over the next ten years.

But this cannot be achieved by Defence alone. Industry plays a critical role in the provision of capabilities and personnel on which Defence relies. Accordingly, Defence and industry must work hand-in-hand to ensure strong cyber security across the Defence ecosystem, and ultimately the success of Defence's warfighting mission.

Defence's approach to cyber security will require ongoing recalibration in the face of an evolving cyber threat environment and rapid technological advancements. This Strategy will continue to be reviewed on an annual basis to ensure currency and to maintain the security of Defence's warfighting capability.


Australian Government
Defence