



DEFENCE CYBER SECURITY STRATEGY



© Commonwealth of Australia 2022

ISBN: XXX

This work is copyright. Apart from use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Department of Defence.

CONTENTS

05	FOREWORD
07	EXECUTIVE SUMMARY
08	Strategic Context
09	Strategic Vision
10	Principles
12	THE PLAN
13	Cyber Security Governance
14	Capability Management
15	People
16	Future Ready
17	WHERE TO FROM HERE?

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 will position Defence to defend Australia and advance our security and prosperity.

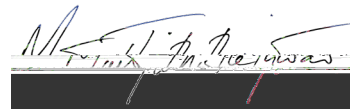
This Strategy details how Defence will combat cyber threats and ensure its capabilities are secure against attacks from adversaries. This will require a concerted and coordinated effort across the entire Defence ecosystem, from Australian Defence Force and Australian Public Service personnel to Defence's 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 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

STRATEGIC CONTEXT

The 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.



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

CYBER SECURITY GOVERNANCE

All of Defence's capabilities operate to some extent in and through cyberspace. This poses

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

28.48 Tm (ndsr).2 (ne (6.8 the 8 (acritical r)utu. 7).3 P Kang (pt-PT)MCID 4 BDC BT80.8 Tw 11 0 02760.

WHERE TO FROM HERE?

This Strategy is designed to deliver on the objectives of the . 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

