Australian Government
Department of Defence

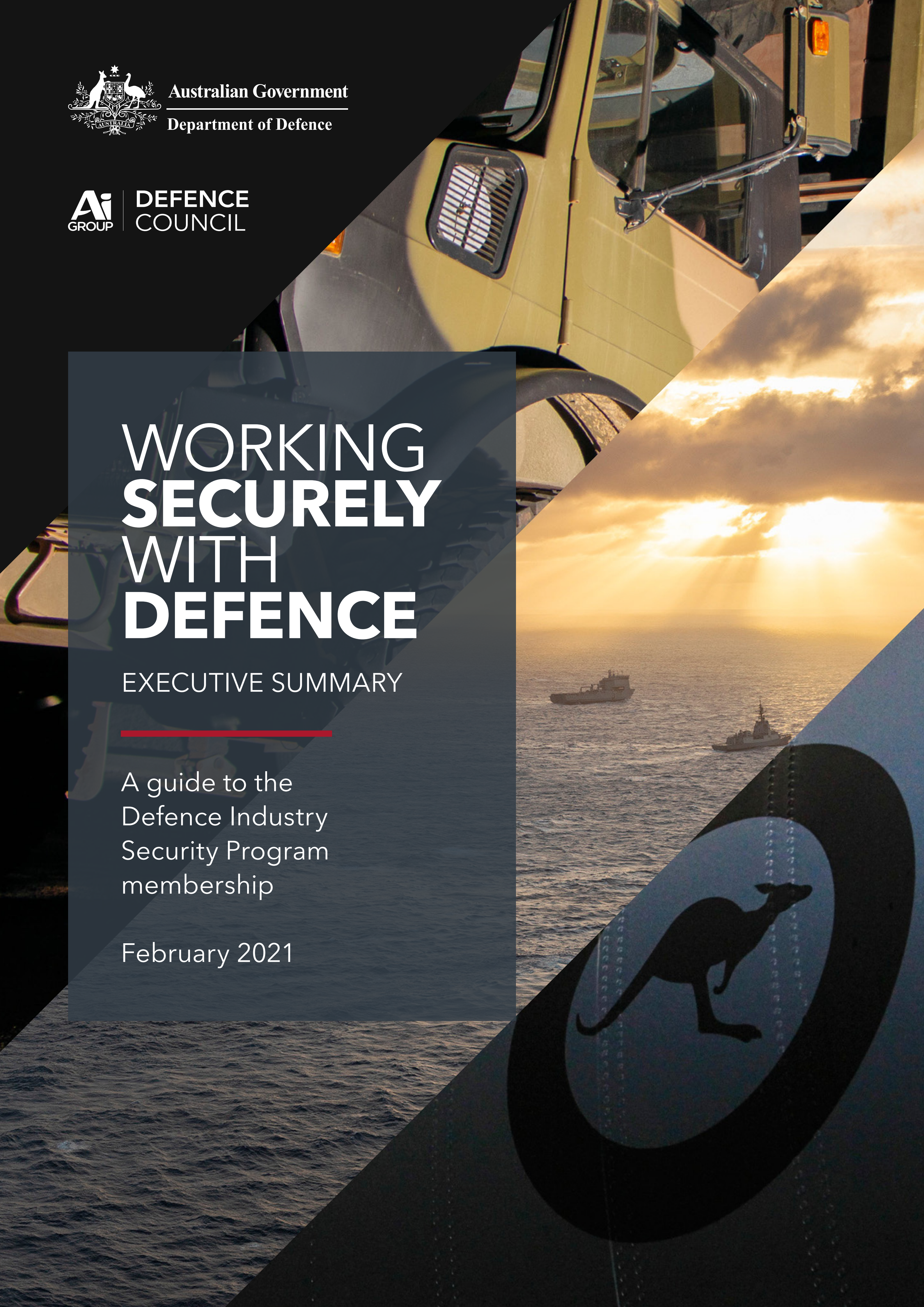
Ai GROUP | DEFENCE COUNCIL

WORKING **SECURELY** WITH **DEFENCE**

EXECUTIVE SUMMARY

A guide to the Defence Industry Security Program membership

February 2021



Executive Summary

The Defence security environment

On 1 July 2020, the Prime Minister announced the 2020 Defence Strategic Update and the 2020 Force Structure Plan. These documents outline a revision to Australia's strategy in responding to evolving challenges and destabilising forces identified in the 2016 Defence White Paper. The realisation of these challenges has been accelerated by a number of factors, including the global coronavirus pandemic. Australia's strategic environment has deteriorated quicker than anticipated. Australia is operating in a period of global transition, seeking to uphold the maintenance of rules based order. To do this, the updates call on Defence to shape Australia's strategic environment, deter actions against Australia's interests and respond with credible military force.

The 2020 Force Structure Plan refers to credible military force in five domains, being the:

1. Information and cyber domain;
2. Maritime domain;
3. Air domain;
4. Space domain; and
5. Land domain.

The expansion of Australia's military capability beyond the tri-service environment, into five domains, represents a significant shift in Australia's military structure. The update demonstrates Australia's move toward military modernisation that is prepared to counter contemporary threats and respond with credible military force. These will enable: competition; increased potency and military endurance; response to grey zone tactics; decisive action in deterrence of threats against Australian interests; values based approach; and sovereign capability.

Australia faces a range of sophisticated and persistent espionage and foreign interference threats from hostile foreign intelligence services, with Defence and associated industry prime targets. We have already experienced alarming breaches and attempted breaches of Defence industry organisations that could impact our nation's safety and future prosperity. Defence and industry have learned from these experiences, however, threats and associated risks are constantly evolving so Defence and industry must too.

There are many things you can do to raise your levels of security protection and minimise your risks. Experts recognise that protective security requirements are multi-layered and interdependent, referred to as Security-in-Depth. Becoming part of the Defence Industry Security Program (DISP) will help ensure you are playing your part in a Security-in-Depth approach.

About the DISP

The revised DISP was launched on 9 April 2019 to meet the requirements of a modern Defence organisation, representing a fundamental change in approach to industry security. Defence continues to improve and update the DISP, through engagement with whole of government stakeholder and industry.

The DISP offers substantial benefits to Defence and industry in streamlining security services and protecting Defence information and assets, as well as industry's intellectual property.

In some instances, DISP membership is mandated by the nature of work delivered to Defence or as a result of a Defence business requirement specified in a contract. For some businesses, DISP membership will not be required, however membership is strongly encouraged to ensure they meet minimum security requirements to engage with Defence at a later stage, or as a demonstration of sound security practice even when handling OFFICIAL information.

The DISP has four membership levels associated with access to the level of information at particular security classifications, which can be tailored to suit your organisation's needs:

	Governance	Personnel Security	Physical Security	ICT and Cyber Security
Entry Level	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive
Level 1	PROTECTED	PROTECTED	PROTECTED	PROTECTED
Level 2	SECRET	SECRET	SECRET	SECRET
Level 3	TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET

Applying for DISP membership

Before starting your application for DISP membership, ensure your business has the following:

- Nominated Chief Security Officer (CSO) and Security Officer (SO) who meet the appropriate DISP level requirement being sought.
- Generic email address for all security related correspondence.
- Ensure that your business ICT network meets a relevant accreditation standard.

Use the following steps to apply for DISP membership

1. Familiarise yourself with ‘Principle 16 and Control 16.1 - Defence Industry Security Program’ of the DSPF: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.
2. Decide which membership levels are most appropriate for the type of work your business provides. At this stage, consider engaging with the Defence contract manager or the DISP team if required. You will also need to build your evidence that demonstrates that you meet the specified requirements for:
   a. Governance
   b. Personnel security
   c. Physical security
   d. ICT and cyber security.
3. Fill out the DISP application form and save to your computer: https://ext.defence.gov.au/security/industry-resources.
4. Fill out the DISP foreign ownership, control and influence declaration form and save to your computer: https://ext.defence.gov.au/security/industry-resources.
5. Email your completed forms to disp.submit@defence.gov.au.

Questions for assessing your capacity to develop your application and build the required evidence

Governance

Does your organisation have a nominated CSO who is accountable for the security of your business?	Yes or No
Does your business have a nominated SO (can be the same person as the CSO)?	Yes or No
If yes, do they have a security clearance and at what level?	Specify personnel security clearance level
Does your business have Security Policies and Plans in place at the appropriate level of DISP membership which will be maintained and made available to Defence upon request?	Yes or No
Does your business run an annual Security Awareness Program for all staff at the appropriate level of DISP membership and is this available to Defence on request?	Yes or No
Does your business have an Insider Threat Awareness program suitable for the level of DISP membership and is this available on request to Defence?	Yes or No
Do the CSO and SO commit to their DISP reporting obligations? This includes maintaining a register of security incident reports, contact reports and overseas travel briefings, and will make this register available to Defence upon request.	Yes or No
Does your business have a mechanism for the governing body, through the CSO, to approve the Annual Security Report and submit this annually?	Yes or No
If you are applying for DISP membership Level 1 or above for personnel security, can you confirm your business maintains a list of Designated Security Assessed Positions, and will make this available to Defence upon request?	Yes or No

Personnel Security

From the time of application for DISP membership, will all future business employment practices meet or exceed the requirements of employment screening standard AS 4811-2006, and be made available to Defence upon request?	Yes or No
Does the SO agree to support the business's security clearance holders to uphold their clearance and compartments responsibilities? This includes, but not limited to: submitting change of circumstances forms, incident reports, contact reports and conducting overseas travel briefings.	Yes or No
Will your people be working in a Defence establishment? If yes, they may need a clearance as specified by the establishment.	Yes or No
Do your employees need a security clearance?	Yes or No

Do any of your personnel have a personnel security clearance?	Yes or No
If yes, what level of personnel security clearance?	Specify level of personnel security clearance

Physical Security

Does your business need to use classified information and/or assets?	Yes or No
What is the highest level of classification your business needs to use?	OFFICIAL OFFICIAL: Sensitive PROTECTED SECRET TOP SECRET
Does your business have clear access control policy and permissions in practice?	Yes or No
Does this extend to any third party providers of goods and services?	Yes or No

Information and Cyber Security

Will your information networks need to handle classified information?	Yes or No
What is the highest level of classified information your business needs to store, process or communicate?	OFFICIAL OFFICIAL: Sensitive PROTECTED SECRET TOP SECRET
Which standard does your business's corporate networks meet?	• Top 4 of the ASD Essential 8 (specifically application control, patch applications, restrict administrative privileges, and patch operating systems) • ISO/IEC 27001 and 27002 • NIST SP 800-171 (US ITAR requirement) • Def Stan 05-138

Once DISP membership has been granted, you may gain access to information on emerging security threats, further guidance to improve and maintain the security of your business, and engage with other members to share lessons learnt.

Other information

The above information does not provide an exhaustive list of the DISP requirements. Users of this Guide should to refer to the relevant sections in this document for further information:

- Chapter 1 discusses the Defence security environment.
- Chapters 2 and 3 explore further about the DISP and considerations when applying for membership.

- Chapters 4 to 7 outline the specific requirements for each of the DISP security categories on governance, personnel security, physical security, and ICT and cyber security, and how to build your evidence in making your DISP applications.
- Chapter 8 summarises ongoing obligations for businesses once they become DISP members.
- Chapter 9 provides further information on being part of the Defence industry supply chain.
- Chapter 10 sets out how to respond to security incidents.

The Guide includes a range of industry tips, case studies, links to relevant resources, assistance, contacts and templates. With input from Defence and industry, all this information has been designed to assist businesses in putting together their DISP applications.

The Guide has also been designed as a companion document to the DISP website and should be read in conjunction with all information provided by Defence. The DISP website will be regularly updated to reflect any changes to policy and regulation and is therefore the primary source of information.

Contact information

For information on DISP membership, contact Defence on:

Phone: 1800 333 362

Email: disp.info@defence.gov.au

Australian Government
Department of Defence

Ai GROUP
DEFENCE COUNCIL

Cover images: Australian Department of Defence © Commonwealth of Australia 2020. Terms and conditions on the use of the images can be found here: https://www1.defence.gov.au/copyright.

DISCLAIMER: The information contained in this document is general in nature, not intended to be relied upon as legal opinion and does not constitute, in any manner, legal advice. Please note that all information is provided 'as is' and is subject to change. The content in this document may be copyrighted, proprietary and subject to intellectual property or other rights of Ai Group and other parties. The authors of this document assume no legal liability or responsibility for the accuracy and completeness of the information and have no liability whatsoever for any errors or omissions in the information, and disclaim all liability howsoever caused (including as a result of negligence), arising from the use of, or reliance on, this publication. By accessing this publication, users are deemed to have consented to this condition and agree that this publication is used entirely at their own risk. In addition, the authors do not guarantee, and accept no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained on any website or on any linked site referred to in this document. We recommend that users exercise their own skill and care with respect to the use of any web site referred to and that users carefully evaluate the accuracy, currency, completeness and relevance of the material on the web site for their specific purposes. Users are encouraged to use the content contained or referred to and to make their own enquiries and assessment of content for their specific purposes. This document is not a substitute for independent professional advice and users should obtain any appropriate professional advice relevant to their particular circumstances.