

# **Independent Review of the Defence Trade Controls Act 2012**

**Dr Vivienne Thom AM**

**October 2018**

© Commonwealth of Australia 2018

ISBN 978-1-925890-01-3 (print)

ISBN 978-1-925890-02-0 (online)

### **Creative Commons Attribution licence**

This publication is available for your use under a Creative Commons Attribution 3.0 Australia licence, with the exception of the signatures, and where otherwise stated.

### **Attribution**

Use of this material under a Creative Commons Attribution 3.0 Australia licence requires you to attribute this report in your work. Any reasonable form of words may be used to attribute the relevant content to this report, provided that it does not in any way suggest that the Department of Defence or the Review of the *Defence Trade Controls Act 2012* endorses you, your work, or your use of the content of this report.



More information about the Creative Commons Attribution 3.0 Australia licence, including the full licence terms, is available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>. Requests and enquiries regarding this licence should be addressed to Defence Publishing Services, Department of Defence.

### **Disclaimer**

Views expressed in this report are those of the independent reviewer or of persons who have provided written submissions to the independent reviewer, and may not reflect the views of the Australian Government, including the Department of Defence.

# LETTER OF TRANSMITTAL

The Hon. Christopher Pyne, MP  
Minister for Defence  
Parliament House  
Canberra ACT 2600

Dear Minister

I am pleased to provide my report of the independent review I have conducted into the *Defence Trade Controls Act 2012* (the DTC Act). The Review addresses its terms of reference.

The Review was established in April 2018 in accordance with section 74B of the DTC Act, which requires that a review of the DTC Act be undertaken two years after the commencement of section 10 of the DTC Act. The same legislative provision requires that you cause a copy of the report to be tabled in each House of Parliament within 15 sitting days after the report is given to you.

In the course of the Review, I received some 75 written submissions and met personally with a wide range of stakeholders, including from government, industry, the research sector, the university sector and peak bodies. I take this opportunity to acknowledge their input.

Finally, for their excellent work, I would like to thank the members of the Review Secretariat for their assistance with logistics, research and the drafting of the report.

Yours sincerely



Dr Vivienne Thom AM  
Independent Reviewer  
19 October 2018

THIS PAGE IS INTENTIONALLY BLANK

# CONTENTS

<b>Letter of Transmittal</b> .....	<b>1</b>
<b>Contents</b> .....	<b>3</b>
<b>Executive summary</b> .....	<b>5</b>
Background .....	5
Administration of the DTC Act .....	5
Gaps in the DTC Act’s controls.....	6
Regulatory overreach .....	8
<b>Glossary</b> .....	<b>9</b>
<b>Part 1: Control of the export of defence-related technology in Australia</b> .....	<b>11</b>
Australia’s export controls.....	11
International arrangements .....	11
Control list and ‘catch-all’ controls.....	12
The DTC Act .....	12
Administration of the DTC Act .....	15
Related legislation .....	17
<b>Part 2: The Review</b> .....	<b>19</b>
Background to the Review .....	19
Consultation .....	19
<b>Part 3: The administration of the DTC Act</b> .....	<b>21</b>
Defence’s administration of the DTC Act.....	21
Interpretation of the DSGL.....	23
Lack of awareness of the DTC Act .....	25
Is a mandatory compliance standard needed? .....	27
Coordination across government.....	27

<b>Part 4: Is the DTC Act fit for purpose? .....</b>	<b>29</b>
Ensuring continued access to allied technology.....	29
A changed national security environment.....	31
Are there gaps in the current legislation? .....	32
How should the gaps be addressed? .....	40
Ensuring a proportionate risk-based approach .....	43
Brokering of controlled goods and technology.....	44
Monitoring and investigation powers.....	45
Functionally equivalent methods of the supply of technology .....	47
 <b>Part 5: Possible regulatory overreach .....</b>	 <b>49</b>
The ‘basic scientific research’ exemption.....	49
Is the current regulation of cryptographic research appropriate? .....	51
Supply to a related body corporate .....	54
Exemptions for ANSTO officers .....	54
 <b>Appendix A: Terms of reference.....</b>	 <b>57</b>
 <b>Appendix B: List of submissions.....</b>	 <b>59</b>
 <b>Appendix C: List of meetings .....</b>	 <b>61</b>

# EXECUTIVE SUMMARY

## BACKGROUND

The *Defence Trade Controls Act 2012* (the DTC Act) provides the legislative basis for the control of the supply, publication and brokering of defence and strategic goods and technology.

The DTC Act was amended in 2015 following extensive stakeholder consultation. The amendments provided for review of the operation of the DTC Act two years after the offence provisions commenced. This is the report of that independent review (the Review).

The Review assessed whether the DTC Act provides appropriate levels of regulation and security for controlled technologies; aligns with international best practice for export controls; and is not unnecessarily restricting trade, research and international collaboration.

The Review engaged in extensive consultation with stakeholders, including the defence industry, research and university sectors.

## ADMINISTRATION OF THE DTC ACT

Stakeholder submissions about the administration of the DTC Act were generally positive, but delay in the processing of applications emerged as a key risk to users. The Review finds that current trends show an increase in processing times, which could adversely affect collaboration and contractual negotiations.

### Recommendation 1

The Department of Defence and other relevant Australian Government agencies should review the processing of *Defence Trade Control Act 2012* applications to ensure that processing times do not continue to exceed standards. The review should include resourcing requirements, particularly in light of any changes that are made to the legislation.

The Defence and Strategic Goods List (DSGL) is a legislative instrument that identifies the goods and technology controlled by the provisions of the DTC Act. Stakeholders require effective supporting and explanatory material to understand the DSGL because of its inherent complexity. The Review finds that current material is not entirely accurate or user-friendly and recommends improvements.

### Recommendation 2

The Department of Defence (Defence) should allocate adequate resources to review the online tool for the Defence and Strategic Goods List (DSGL) in order to enhance the tool's accuracy and utility for researchers and other stakeholders. Defence should also consider developing other explanatory materials relating to the DSGL, including improved online training and refreshed case studies.

A consistent concern that emerged in discussions with stakeholders was the general lack of awareness of the existence of the DTC Act, its objectives and its application in key sectors. While Defence does conduct outreach activities, the program should be targeted at key sectors and could be delivered by partnering with other relevant bodies.

### Recommendation 3

The Department of Defence (Defence) should allocate adequate resources to develop and deliver an effective program to ensure that key sectors, including university researchers and small and medium enterprises, are aware of their obligations under the *Defence Trade Controls Act 2012*. Defence should also explore partnering with other government or industry bodies to raise awareness.

## GAPS IN THE DTC ACT'S CONTROLS

Defence advised the Review that the national security environment had changed since the DTC Act was implemented and that current provisions were not sufficient to protect Australia's national interests. Defence made recommendations to strengthen the controls in the DTC Act. Other stakeholders expressed significant concerns with Defence's proposal.

The Review recognises that changes in the national security environment require that the legislation be amended in order for it to remain effective, but does not support the broad approach implied by the recommendations in the Defence submission.

The Review supports the proposition that direct and ongoing consultation is required between Defence and stakeholders to develop a policy proposal that takes a proportionate approach to address the current gaps in the legislation but also addresses the serious and legitimate concerns of industry, research bodies and universities. Any solution must focus effort and resources on protecting technology that would cause the most damage should it be obtained by foreign entities that may use it against Australian interests.

While it would be premature for the Review to formulate any prescriptive recommendations for legislative amendments, it is appropriate to articulate principles that could guide such changes.

### Recommendation 4

The Department of Defence should work with stakeholders to develop a practical legislative proposal to address the following gaps in the *Defence Trade Controls Act 2012* (DTC Act):

- the limitation of the supply provision at section 10 that specifies that it applies only when certain locational criteria are met at the time of supply
- the lack of control over the transfer of technology not captured by the DTC Act's existing provisions but which, if transferred to foreign entities with interests contrary to Australia's, could prejudice Australia's security, defence and international relations
- the inadequate control of emerging and sensitive military and dual-use technology.

To ensure that any amendment does not unnecessarily restrict trade, research and international collaboration, the legislative proposal should:

- ensure all decisions are targeted and based on risk-related consideration of the technology being supplied, the end user and the end use
- contain measures to ensure transparency and scrutiny of decisions
- limit additional uncertainty, complexity and risk of inadvertent breaches
- minimise any increased compliance costs.

The Review makes three additional recommendations to remedy deficiencies in the DTC Act. The first relates to a possible uncertainty in the scope of the brokering provision which may currently allow a person to avoid the provisions of the Act by using certain contractual arrangements.

## Recommendation 5

The Government should consider amending the definition of ‘arranging for persons to supply goods or DSSL technology’ (that is, ‘brokering’) in the *Defence Trade Controls Act 2012* to ensure that the provision clearly reflects the objectives of the Act. Any amendment to the legislation should be communicated effectively to affected entities.

The Review was also persuaded that Defence should be given appropriate powers to monitor compliance, or to effectively investigate suspected non-compliance, to determine whether cases should be referred to the Australian Federal Police or administrative compliance action should be taken.

## Recommendation 6

The Government should consider triggering the general monitoring and investigation powers set out in *Regulatory Powers (Standard Provisions) Act 2014* for use by the Department of Defence to monitor and investigate compliance with the *Defence Trade Controls Act 2012* and ensure that additional properly trained staff are allocated to exercise these powers.

A number of stakeholders pointed to apparent inconsistencies in the DTC Act that could lead to avoidance of the DTC Act’s controls by the use of different technical methods for supply or publication. The Review recommends that the Government should consider how the controls could be tightened to address these apparent gaps.

## Recommendation 7

The Government should consider amending the *Defence Trade Controls Act 2012* to ensure that the Act’s objectives are achieved by ensuring that the regulation is independent of the technical method used to supply or publish technology.

## REGULATORY OVERREACH

Submissions from the research and university sectors suggest that the 'basic scientific research' exemption in the DSGL is not aligned with the export controls of like-minded partners. While the Review accepts that the exemptions in Australia may not align exactly with those in the United States, the Review was not persuaded that a case to amend the 'basic scientific research' exemption has been made out at this stage.

The Review also considered stakeholder submissions that the controls in the DTC Act should not apply to cryptographic research. The Review does not find that a case for legislative amendment has been made at this stage but recommends that Defence consider this option when it reviews the outcome of its current cryptography permit trial.

### Recommendation 8

The Department of Defence should formally evaluate its two-step cryptography permit trial and decide whether the approach will be implemented on an ongoing basis. The evaluation should consider whether an alternative approach would be preferable and explore whether the clarification of existing thresholds would be sufficient or whether legislative amendment is required.

The Review accepts a submission by the Australian Nuclear Science and Technology Organisation that certain offence exemptions that currently apply to specified classes of Australian Government officials should also apply to its employees where the activities occur in the course of their duties.

### Recommendation 9

The Government should consider amending the *Defence Trade Controls Act 2012* to include employees of the Australian Nuclear Science and Technology Organisation in the offence exemptions of sections 10(3) and 15, where the activities occur in the course of their duties.

# GLOSSARY

ADF	Australian Defence Force
ANSTO	Australian Nuclear Science and Technology Organisation
BIS	United States Department of Commerce, Bureau of Industry and Security
CCL	Commerce Control List
controlled goods or technology	goods or technology specified in the DSGL
Customs PE Regulations	Customs (Prohibited Exports) Regulations 1958
DEC	Defence Exports Controls
Defence	Department of Defence
DFAT	The Department of Foreign Affairs and Trade
DSGL	Defence and Strategic Goods List
DTC Act	<i>Defence Trade Controls Act 2012</i>
DTC Bill	Defence Trade Controls Bill 2011
dual-use goods or technology	goods or technology developed for primarily a commercial application but also have application in a military context
EAR	Export Administration Regulations (US)
ITAR	International Traffic in Arms Regulations (US)
military goods or technology	goods or technology developed specifically for military use
RP Act	<i>Regulatory Powers (Standard Provisions) Act 2014</i>
SME	small and medium enterprise
TRL	technology readiness level
USML	US Munitions List
WMD	Weapons of Mass Destruction

THIS PAGE IS INTENTIONALLY BLANK

# PART 1: CONTROL OF THE EXPORT OF DEFENCE-RELATED TECHNOLOGY IN AUSTRALIA

## AUSTRALIA'S EXPORT CONTROLS

Australia's export control system aims to stop military goods and technology—and goods and technology that can be used in chemical, biological and nuclear weapons—from being transferred to individuals, states or groups with interests prejudicial to Australian interests. As a member of international export control regimes, Australia is part of a global effort to regulate the export of items controlled by these regimes, which have military or weapons of mass destruction (WMD) applications. The *Defence Trade Controls Act 2012* (the DTC Act) forms part of a wider export control framework.<sup>1</sup>

## INTERNATIONAL ARRANGEMENTS

Australia is a signatory to a number of international arms control treaties and an active member of the four main multilateral export control regimes:

- Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement)<sup>2</sup>
- Australia Group on chemical and biological weapons materials<sup>3</sup>
- Nuclear Suppliers Group for nuclear and nuclear related goods<sup>4</sup>
- Missile Technology Control Regime for ballistic missiles and other WMD delivery systems.<sup>5</sup>

The export control regimes have the common objective—through the coordination of national export control policies—of controlling the export of goods and technology that can be used in:

- WMD and their delivery systems
- conventional weapons or components thereof
- dual-use goods that can have a military or security application.

This is achieved through the implementation by member countries of specific measures and trade control lists developed by each regime. Member countries undertake to regulate the trade on controlled goods and technology, and on goods and technology with a military or WMD end use, through national laws, which established systems to regulate their export and transfer.

Like-minded countries, including the United States, United Kingdom, Canada, New Zealand, Japan and the European Union nations, are members of the four export control regimes and have similar regulations and control lists to those of Australia.

---

1 <http://www.defence.gov.au/ExportControls/Legislation.asp>.

2 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, *Introduction*, <https://www.wassenaar.org/>.

3 The Australia Group, [www.australiagroup.net/](http://www.australiagroup.net/).

4 Nuclear Suppliers Group, *About the NSG*, [www.nuclearsuppliersgroup.org/en/](http://www.nuclearsuppliersgroup.org/en/).

5 Missile Technology Control Regime, <http://mtcr.info/>.

## CONTROL LIST AND ‘CATCH-ALL’ CONTROLS

The four export control regimes each have control lists of goods and technologies to which member countries’ export control regulations apply.<sup>6</sup> Consequently, the control lists of all members generally reflect each other, although some variations occur.

Australia’s list of controlled goods and technologies is the Defence and Strategic Goods List (DSGL). The DSGL is a legislative instrument that lists controlled goods and technology that are regulated in Australia by the DTC Act and the Customs (Prohibited Exports) Regulations 1958 (Customs PE Regulations). The DTC Act regulates the supply, publication and brokering of DSGL technology and goods. The Customs PE Regulations regulates the export of DSGL goods.

The DSGL is divided into two parts: Part 1 includes military goods and technology, and Part 2 includes dual-use goods and technology. Military goods and technology are items, including parts and accessories, that are specifically designed for military or lethal use. Dual-use goods and technology are designed for a commercial purpose but can be used either as military components or for the development, production or use of military systems or WMD. Items are excluded from control if they are considered ‘basic scientific research’ or are already in the public domain.<sup>7</sup>

In the context of the DSGL and the controls, the term ‘technology’ means specific information necessary for the ‘development’, ‘production’ or ‘use’ of a product. ‘Information’ can be either ‘technical data’ or ‘technical assistance’.<sup>8</sup>

In addition to controlling the export or supply of goods and technology listed on the DSGL, Australia has legislation that allows the Minister for Defence to regulate the export of any goods or technology when the Minister is satisfied that those goods or technology could be used in a WMD program or for a military end use. These provisions are referred to as ‘catch-all controls’.<sup>9</sup>

## THE DTC ACT

### Background to the DTC Act

Prior to 2016, the export of goods and technology listed on the DSGL was largely regulated by regulation 13E of the Customs PE Regulations only. Exporters were required to obtain a permit before exporting DSGL goods. DSGL technology was largely unregulated; a permit was required only to export technology stored on a good, such as on a USB or hard drive. If an export was assessed as not in the national interest, the Minister for Defence had the power to refuse to issue a permit, and the export could not legally proceed. Electronic transfer of DSGL technology was unregulated.

6 Missile Technology Control Regime, *MTCR Annex Handbook*, <http://mtcr.info/mtcr-annex/>; Australia Group, *Australia Group Common Control Lists*, <https://australiagroup.net/en/controllists.html>; Nuclear Suppliers Group, *Guidelines*, <http://www.nuclearsuppliersgroup.org/en/guidelines>; Wassenaar Arrangement, *Control Lists*, <https://www.wassenaar.org/control-lists/>.

7 Department of Defence, *Defence Export Controls*, *The Defence and Strategic Goods List*, <http://www.defence.gov.au/ExportControls/DSGL.asp>.

8 Defence and Strategic Goods List, Division 4, <https://www.legislation.gov.au/Details/F2016C00970>.

9 Section 112BA of the *Customs Act 1901* and *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995*.

In 2003 and 2006, the Wassenaar Arrangement participating states agreed that, in addition to regulating the export of controlled goods, they should also regulate brokering in controlled goods and technology and the electronic, or intangible, transfer of controlled technology. The regimes drafted and accepted best practice guidance for member countries.<sup>10</sup> The guidance advised best practice controls on intangible transfers of technology. Also, during this period, the regimes identified the control of international brokering activities as important for achieving export control aims.

In 2012, the Defence Trade Controls Bill 2011 (DTC Bill) proposed controls on the 'supply' and 'publishing' of DSGL technology and the 'brokering' of DSGL goods and technology. The DTC Bill implemented, in accordance with the national interest at the time, the commitments Australia had made as a member country in the export control regimes.

Stakeholders, most notably the research and university sectors, raised several concerns about the regulatory impact of the DTC Bill. Researchers' core business relies on the free and open sharing of technology and information; they routinely collaborate with foreign partners and communicate ideas and developments electronically. Consequently, the sector was concerned about the significant regulatory burden the DTC Act would place on its activities, the impact of the controls on academic freedom and its ability to comply.<sup>11</sup>

In response to stakeholder concerns, the DTC Bill was amended to include a provision that delayed the commencement of the offence provisions. A steering group was established to advise the Minister for Defence and the Research Minister (then the Minister for Industry and Science) whether the controls fulfilled Australia's international obligations and national interest requirements without unnecessarily restricting trade, research and international collaboration or reducing the international competitiveness of the research sector.<sup>12</sup>

The Department of Defence (Defence), the steering group and stakeholders worked closely together to address stakeholders' concerns with the DTC Act. The steering group accepted that the DTC Act did not strike an appropriate balance between national security and regulatory burden. The steering group recommended amendment of the DTC Act to adopt a more risk-based approach and the implementation of policy changes to streamline the controls and reduce regulation.<sup>13</sup>

The risk-based approach included removing permit requirements for activities assessed as low risk at that time, limiting the control of oral supply of DSGL technology, and limiting brokering and publication controls to military goods and technology only (that is, Part 1 of the DSGL). The recommendations were accepted, and amendments to the DTC Act were made by the *Defence Trade Controls Amendment Act 2015* (DTC Amendment Act).

---

10 Wassenaar Arrangement, *Best practices and guidelines*, <https://www.wassenaar.org/best-practices/>.

11 Senate Foreign Affairs, Defence and Trade Legislation Committee, *Defence Trade Control Bill 2011 [Provisions]*, October 2012, pp 7–13.

12 Department of Defence, Defence Export Controls, *Strengthened Export Controls Steering Group*, <http://www.defence.gov.au/ExportControls/Steering.asp>.

13 Department of Defence, Defence Export Controls, *Public Communique March 2015*, <http://www.defence.gov.au/ExportControls/ECSC/index.html>.

## Overview of the DTC Act

The DTC Act regulates the:

- supply of, or the provision of access to, DSGL technology from a place in Australia to 'another person' in a place outside Australia
- oral supply of DSGL technology that is for a military end use or WMD end use
- brokering of DSGL Part 1 goods and technology
- brokering of goods or DSGL technology when it may be for a military end use
- publication of DSGL Part 1 technology.

The DTC Act also includes non-delegable powers that allow the Minister for Defence to prohibit certain activities when the Minister reasonably believes the activity would prejudice the security, defence or international relations of Australia (catch-all controls). The Minister may notify a person that an activity is prohibited by giving them a written notice.

These prohibition powers include:

- prohibiting a person from supplying DSGL technology in any circumstance (section 14)
- prohibiting a person from publishing DSGL technology to the public or a specified section of the public (section 14B)
- prohibiting a person from arranging the supply of DSGL goods or DSGL technology (section 15A).

The DTC Act includes offences for persons who do certain activities without, or not in accordance with, a permit or approval given under the DTC Act.

The DTC Act provides that the Secretary for Defence may obtain information from a person or documents that are relevant to the operation of the DTC Act. Persons who hold permits under the DTC Act are required to keep certain records.

## ADMINISTRATION OF THE DTC ACT

Applications for permits under the DTC Act are assessed on a case-by-case basis by Defence Export Controls Branch (DEC) in Defence. Section 11 of the DTC Act allows the Minister (or delegate) to give a person a permit if they are satisfied that the supply of DSGL technology would not prejudice the security, defence or international relations of Australia (section 16 includes a similar provision for brokering permits). In practice, when assessing an application for a permit, Defence considers:

- the goods, technology or services being supplied or provided
- the destination
- the end use
- the end user.<sup>14</sup>

The assessment looks to verify the authenticity of the parties associated with the application, the information presented or omitted from the application, the supporting documentation provided, the stated end use of the goods and whether the stated end use fits with the primary business activities of the stated end user.

If Defence forms a preliminary assessment that a supply, publication or brokering activity might be contrary to the national interest, it consults with other government agencies, including the Department of Foreign Affairs and Trade (DFAT), that may provide advice on the final outcome.

When assessing applications, Defence, often in consultation with other relevant government agencies, assesses the implications of the supply, publication or brokering activity against specific criteria to determine whether the activity may be prejudicial to the security, defence or international relations of Australia. Twelve broad criteria are set out in regulation 8 of the Defence Trade Controls Regulation 2013:

1. The risk that the DSGL technology or the goods may go to or become available to a country upon which the Security Council of the United Nations or Australia has imposed a sanction
2. The risk that the DSGL technology or the goods may go to or become available to a country where it may be used in a way contrary to Australia's international obligations or commitments
3. The risk that the DSGL technology or the goods may be used to commit or facilitate serious abuses of human rights
4. Whether the supply of the DSGL technology or the goods, or the publication of the DSGL technology:
  - (a) may aggravate:
    - (i) an existing threat to international peace and security or to the peace and security of a region; or
    - (ii) a particular event or conflict of concern to Australia; or
  - (b) may otherwise contribute to political instability internationally or in a particular region
5. Whether the DSGL technology or the goods may:
  - (a) be used for conflict within a country or for international conflict by a country; or
  - (b) further militarise conflict within a country

---

<sup>14</sup> Department of Defence, Defence Export Controls, *Assessment process*, <http://defence.gov.au/ExportControls/Assessment.asp>.

6. Whether the supply of the DSGL technology or the goods, or the publication of the DSGL technology, may compromise or adversely affect Australia's defence or security interests, its obligations to its allies or its international obligations and responsibilities
7. Whether the DSGL technology or the goods may go to or become available to a country that has policies or strategic interests that are inconsistent with the policies and strategic interests of Australia or its allies
8. The risk that the supply of the DSGL technology or the goods, or the publication of the DSGL technology, may:
  - (a) adversely affect Australia's military capability; or
  - (b) substantially compromise an Australian defence operation; or
  - (c) increase the military capability of a country that is a potential adversary of Australia
9. The risk that the DSGL technology or the goods may go to or become available to a country:
  - (a) that is developing, or is reasonably suspected of developing:
    - (i) weapons that may be capable of causing mass destruction; or
    - (ii) the means of delivering such weapons; or
  - (b) that supports, or is reasonably suspected of supporting, terrorism; or
  - (c) whose actions or foreign policies pose a risk of major disruption in global stability or the stability of a particular region
10. Whether the supply of the DSGL technology or the goods, or the publication of the DSGL technology, may lead to a reaction by another country that may damage Australia's interests or relations with the other country or with a particular region
11. Whether the DSGL technology or the goods may be used for mercenary activities or a terrorist or other criminal activity
12. Whether preventing the supply of the DSGL technology or the goods, or the publication of the DSGL technology, may have an adverse effect on Australian industry, trade and economic prosperity to the extent that it may adversely affect the security, defence or international relations of Australia. Following the assessment process, including consultation with other government agencies if required, a recommendation is then made to the Minister for Defence or a delegate for decision. Only the Minister for Defence may refuse to issue a permit.

## RELATED LEGISLATION

### ***The Customs Act 1901***

The Customs PE Regulations, made under the *Customs Act 1901* (the Customs Act), control the export of goods listed on the DSGL. Section 112BA of the Customs Act is a 'catch-all control' that provides the Minister for Defence with the power to prohibit the export of a good not on the DSGL that may be for a military end use that would prejudice the security, defence or international relations of Australia.

### ***The Weapons of Mass Destruction (Prevention of Proliferation) Act 1995***

The *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995* (WMD Act) is a 'catch-all control' that gives the Minister for Defence the power to prohibit the export and supply of goods, the export of otherwise non-regulated goods (that is, goods not regulated by the Customs Act) and the provision of services when the Minister believes or suspects that goods or services would or might be used in, or assist, a WMD program.

### ***Charter of the United Nations Act 1945 and the Autonomous Sanctions Act 2011***

Australia gives effect to United Nations sanctions regimes under the *Charter of the United Nations Act 1945*. There are separate regulations under the DTC Act for each United Nations sanctions regime. Australian autonomous sanctions regimes are implemented under the *Autonomous Sanctions Act 2011*.

DFAT administers the Charter of the United Nations Act and the Autonomous Sanctions Act. The United Nations Act, the Autonomous Act and their regulations use common terms to describe sanctions measures.<sup>15</sup> Sanctions measures may include general prohibitions on:

- making a 'sanctioned supply' of 'export sanctioned goods'
- making a 'sanctioned import' of 'import sanctioned goods'
- providing a 'sanctioned service'
- engaging in a 'sanctioned commercial activity'
- dealing with a 'designated person or entity'
- using or dealing with a 'controlled asset'
- the entry into, or transit through, Australia of a 'designated person' or a 'declared person'.

---

<sup>15</sup> Department of Foreign Affairs and Trade, *About Sanctions*, <https://dfat.gov.au/international-relations/security/sanctions/Pages/about-sanctions.aspx>.

THIS PAGE IS INTENTIONALLY BLANK

# PART 2: THE REVIEW

## BACKGROUND TO THE REVIEW

The DTC Act underwent amendments in 2015 following extensive stakeholder consultation. One of the amendments included the addition of a mechanism to provide for review of the operation of the DTC Act two years after the offence provisions commenced, which occurred on 2 April 2016. The requirements for the Review are set out in section 74B. The scope of the Review excludes Parts 3 and 4 of the DTC Act, which relate to the Defence Trade Cooperation Treaty between Australia and the United States.

On 20 April 2018, the then Minister for Defence, Senator the Hon. Marise Payne, announced that Dr Vivienne Thom AM had been appointed to conduct a review of the DTC Act (the Review). The terms of reference for the Review are set out in Appendix A.

In particular, the Review was to evaluate the operation of the DTC Act and deliver recommendations that ensure the DTC Act is an effective component of Australia's export control regime and appropriately addresses current and future national security requirements.

The Review also aimed to assess whether the DTC Act provides appropriate levels of regulation to ensure the security of defence technologies; aligns with international best practice for export controls; and is not unnecessarily restricting trade, research and international collaboration.

Under section 74B, the reviewer is required to present a report to the Minister for Defence, and a copy of the report must be tabled in each house of the Commonwealth Parliament within 15 sitting days.

## CONSULTATION

The consultation and development experiences leading up to the passage of the DTC Act and the DTC Amendment Act indicated that stakeholder engagement and consultation would be key requirements of the Review and are emphasised in the terms of reference (see Appendix A).

The Review was advertised in *The Weekend Australian* on 28 April and 5 May 2018, with a call for written submissions by 31 May 2018.

Information about the Review and the call for submissions was also communicated to stakeholders and the public through an email alert to approximately 10 000 clients and stakeholders of DEC. Information was also provided to all stakeholders who had made submissions to the Senate Standing Committee on Foreign Affairs, Defence and Trade Inquiry into the Defence Trade Controls Bill 2011<sup>16</sup> or its Inquiry into the Implementation of the *Defence Trade Controls Amendment Act 2015*<sup>17</sup>, or any other consultation process Defence had undertaken to amend export control legislation.

16 Senate Foreign Affairs, Defence and Trade Legislation Committee, *Defence Trade Control Bill 2011 [Provisions]*, Submissions, [https://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Foreign\\_Affairs\\_Defence\\_and\\_Trade/Completed\\_inquiries/2010-13/tradecontrols/submissions](https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/Completed_inquiries/2010-13/tradecontrols/submissions).

17 Senate Foreign Affairs, Defence and Trade Legislation Committee, *Implementation of the Defence Trade Controls Legislation*, Submissions, [https://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Foreign\\_Affairs\\_Defence\\_and\\_Trade/Trade\\_Implementation/Submissions](https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/Trade_Implementation/Submissions).

Forty-six written submissions were received in the first round of public consultation, and these were published on the Review's public website.<sup>18</sup> Submissions were received from the following:

- the university sector and research bodies
- peak bodies
- defence industry prime contractors
- small to medium enterprises
- government agencies and departments
- members of the public.

In response to the significant issues raised in the first round of consultation, the Review invited stakeholders to submit supplementary submissions. This invitation was communicated directly to relevant stakeholders and via a notice on the Review website. Twenty-nine further submissions were received, including 20 supplementary submissions. A list of submissions received is at Appendix B.

The Review conducted 12 stakeholder roundtable discussions in state capitals from 6 to 28 August 2018 to further explore the issues raised in the written submissions.

The Review met with industry, research and university sectors and peak bodies to discuss the Review and encourage all sectors to raise any issues in evidence-based submissions. The Review also met with the relevant federal ministers or their staff and with senior officials from relevant government departments. A list of meetings held is at Appendix C.

---

<sup>18</sup> Department of Defence, Defence Trade Controls Review, *Submissions*, <http://www.defence.gov.au/publications/reviews/tradecontrols/Submissions.asp>.

# PART 3: THE ADMINISTRATION OF THE DTC ACT

## DEFENCE'S ADMINISTRATION OF THE DTC ACT

Overwhelmingly, feedback indicated the support that Defence provides to stakeholders in assisting them to comply with the DTC Act is very good. Comments included that the proactive and professional manner in which DEC assisted institutions to prepare for the DTC Act meant that the expected adverse impacts had been minimised.<sup>19</sup> Defence staff were described as responsive, approachable, well informed and helpful. University stakeholders particularly appreciated the direct points of contact they had been assigned.

Stakeholders advised that the timelines for application assessments and granting of permits are critical to reducing regulatory impact and facilitating collaboration. Generally, the current timeframes were seen as acceptable, but some concerns were expressed about some longer processing times that could affect the ability of universities to enter research contracts within preferred timeframes.<sup>20</sup> Even a delay of two weeks can severely affect a 12-week collaborative project. The Export Council of Australia also commented on the commercial impact of delays.<sup>21</sup>

Saab Australia Pty Ltd (Saab) suggested that DEC should take steps to ensure a strong triage culture or greater resources within DEC to process requests through risk-based assessments faster, including by closely reviewing what technical data is actually being transferred.<sup>22</sup>

The Defence website provides the following standards for processing times:

Other than in exceptional circumstances, the assessment time for routine applications is up to 15 working days (commencing from the date a complete application, with all supporting documentation, is received). For applications requiring referral to other agencies, the assessment time is up to 35 working days and sometimes longer for highly complex applications. We will inform you if your application is referred to another agency.<sup>23</sup>

Defence publishes aggregated workload and performance data on its website.<sup>24</sup> It provided to the Review its data for the processing times for finalised applications (see Table 1). The data in Table 1 does not distinguish between the time taken by DEC and the time taken by other agencies, because it is the total time that is important to stakeholders. An increasing trend has been observed in the number of applications that are not finalised within the published standards, with 24 applications exceeding the maximum standard by more than 5 days in 2017 (taking more than 40 days to be finalised compared with a standard of 35 days for complex cases).

19 University of Tasmania, submission 10, p. 1.

20 Group of Eight, submission 28, p. 2.

21 Export Council of Australia, submission 31, p. 2.

22 Saab Australia Pty Ltd, supplementary submission 19, p. 3.

23 Department of Defence, Defence Export Controls, *Application Process*, <http://www.defence.gov.au/ExportControls/ApplicationProcess.asp>.

24 Department of Defence, Defence Export Controls, *DEC Statistics*, <http://www.defence.gov.au/ExportControls/statistics.asp>.

**Table 1: Processing time for finalised DTC Act applications**

Period		Number of finalised applications	Number of finalised applications with processing times exceeding standards	Number of finalised applications with processing times exceeding 40 working days
2016	Q2	70	12	1
	Q3	69	13	4
	Q4	44	6	2
	<b>Total</b>	<b>183</b>	<b>31</b>	<b>7</b>
2017	Q1	50	3	4
	Q2	49	5	6
	Q3	58	12	4
	Q4	61	11	10
	<b>Total</b>	<b>218</b>	<b>31</b>	<b>24</b>
2018	Q1	64	7	2
	Q2	67	27	7
	Q3 (incomplete)	38	10	2
	<b>Total</b>	<b>169</b>	<b>44</b>	<b>11</b>

The Review recognises that the processing of applications can be complex and may rely on specialised staff, but delays can have serious adverse effects, as set out above. Defence and other relevant agencies should monitor and review the processing of DTC Act applications and processes to ensure that processing times do not continue to exceed standards. Resourcing requirements, particularly in light of any changes that are made to the legislation, should also be reviewed.

### Recommendation 1

The Department of Defence and other relevant Australian Government agencies should review the processing of *Defence Trade Control Act 2012* applications to ensure that processing times do not continue to exceed standards. The review should include resourcing requirements, particularly in light of any changes that are made to the legislation.

## INTERPRETATION OF THE DSGL

The DSGL is a legislative instrument that identifies the goods, software and technology that are controlled by the provisions of the DTC Act (and by the Customs PE Regulations). The items on the list are agreed upon in conjunction with the other member states of the multilateral export control regimes.

The controls specified in the DSGL are complex. To establish whether an item is controlled, a person must establish whether the good is listed, noting that the related equipment, materials or technology may also be listed. If a good or technology is listed on the DSGL, the associated technical parameters and/or specifications and/or performance of the item must also fall within the scope of the DSGL. For many items, the associated technology will only be captured if it is 'required' for the 'development', 'production' or, in some cases, 'use' of the controlled item. Although technology captured by the DSGL is, in most cases, directly linked to a DSGL good, in some cases technology may be captured in its own right—that is, it may not be related to a DSGL good but may still be controlled. The DSGL also applies several exemptions to technology that would otherwise be controlled.<sup>25</sup>

Defence has developed a DSGL online tool to assist people to determine whether a good, software or technology is on the DSGL and whether the activity they plan to undertake in relation to the good or technology is controlled.<sup>26</sup>

The DSGL tool has two parts:

- The Activity Questionnaire is a self-assessment tool that assists in determining whether a supply, publication or brokering activity is controlled by the DTC Act.
- The DSGL Search is a tool that assists in determining whether goods, software or technology are listed on the DSGL.

If, after using the tool, clients still cannot determine whether the good or technology is controlled, they may apply for a DSGL assessment, and a DEC technical assessor will provide authoritative advice on the control status of the good, software or technology.<sup>27</sup>

Stakeholders raised concerns about the difficulty in interpreting the DSGL and the lack of effective supporting tools. Submissions from industry and from the research and university sectors confirmed that the technical and legal language in the DSGL can be difficult to interpret.<sup>28</sup> Thales Australia Limited (Thales) submitted that the thresholds for technical data can be difficult to identify, which presents difficulties in business negotiations.<sup>29</sup> The lack of clarity in DSGL definitions and interpretations could also result in unnecessary applications and an increased administrative burden on both the applicant and DEC.

The Australian National University suggested using technology readiness levels (TRLs) to clarify the DSGL control threshold.<sup>30</sup> This was supported by submissions from the Australasian Research Management Society and the University of Melbourne.<sup>31</sup> TRLs were developed by NASA to measure the maturity of

25 Department of Defence, Defence Export Controls, *The Defence and Strategic Goods List*, <http://www.defence.gov.au/ExportControls/DSGL.asp>.

26 Department of Defence, Defence Export Controls, *Online DSGL Tool*, <https://dsgl.defence.gov.au/Pages/Home.aspx>.

27 Department of Defence, Defence Export Controls, *Application for DSGL Assessment*, <http://www.defence.gov.au/ExportControls/FormDSGLAssess.asp>.

28 See, for example, Queensland University of Technology, submission 33, p. 1; University of South Australia, submission 47, pp. 1–2.

29 Thales Australia Limited, submission 40, pp. 1–2.

30 Australian National University, submission 27, p. 2.

31 Australasian Research Management Society, submission 18, p. 1; University of Melbourne, submission 24, p. 1.

technology and are commonly used in the research and university sectors.<sup>32</sup> However, TRLs are a subjective measure and do not directly align with the control threshold. As such, they can be used as a general indication of the development level and thus whether the technology is approaching a control threshold, but do not provide sufficient clarity to define the control threshold itself.<sup>33</sup>

Queensland University of Technology submitted that DSGL interpretation training delivered online could help to resolve the DSGL interpretation difficulties. It suggested an online course on control thresholds to complement the existing DSGL online tool provided by DEC.<sup>34</sup>

The University of South Australia and other university sector stakeholders commented that although the DSGL online tool is useful for providing cross-referenced information compared to the full DSGL, it has a narrow focus and requires exact wording for successful searches.<sup>35</sup> For example, using the DSGL online tool to search for 'reflectometer' and 'reflectometry' produces no results, suggesting the goods are not controlled. However, searching for 'reflectometers' (plural) produces four results for controlled goods on the DSGL.<sup>36</sup> These false negatives could lead to researchers incorrectly (but not unreasonably) reaching the wrong conclusion about whether particular types of technology are on the DSGL.

Any improvements to assist users to interpret the DSGL could provide efficiencies for Defence as well as for users. For example, Defence could publish case studies to provide step-by-step examples of technical assessments and how DEC assessors decide whether technology is at a threshold that it is necessary for the 'use', 'development' or 'production' of a product.

Stakeholders require effective supporting and explanatory material to understand the DSGL because of its inherent complexity. The DSGL online tool appears to be a valuable supplementary tool that is utilised extensively by stakeholders, despite its current limitations. Modifying the online tool to reflect modern searching conventions and improve the cross-referencing and relevance could further address these limitations.

## Recommendation 2

The Department of Defence (Defence) should allocate adequate resources to review the online tool for the Defence and Strategic Goods List (DSGL) in order to enhance the tool's accuracy and utility for researchers and other stakeholders. Defence should also consider developing other explanatory materials relating to the DSGL, including improved online training and refreshed case studies.

A number of submissions commented on the appropriateness of the inclusion of specific goods or technologies on the DSGL.<sup>37</sup> These matters would be more appropriately considered by Defence in its ongoing revision of the DSGL and are not within the scope of this Review.

32 National Aeronautics and Space Administration, *Technology Readiness Level*, [https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt\\_accordion1.html](https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html).

33 Advice received from DEC technical assessors, Department of Defence, 3 August 2018.

34 Queensland University of Technology, submission 33, p. 1.

35 Issue raised at the Sydney, Melbourne, Adelaide and Perth research-sector stakeholder roundtables.

36 University of South Australia, submission 47, p. 1.

37 See, for example, Morgan Advanced Materials, submission 4, p. 1; Rafael Advanced Defense Systems Ltd, submission 6, p. 1.

## LACK OF AWARENESS OF THE DTC ACT

A consistent concern that emerged in discussions with stakeholders was the general lack of awareness of the existence of the DTC Act, its objectives and its application in key sectors.

Defence currently runs a program of outreach events to increase awareness of defence export controls. Outreach sessions are held annually in most capital cities and involve an introduction to export controls followed by separate specialised sessions for universities and industry, where participants can raise particular issues with DEC officials. Representatives from other government agencies, including the Australian Border Force, the Australian Security Intelligence Organisation and DFAT, regularly attend and provide participants with an overview of their role in the whole-of-government effort to safeguard defence and security capability, implement counter-proliferation and enforce United Nations and autonomous sanctions. The outreach events provide introductory information on export controls; they are promoted on the DEC public website and to those who have had prior contact with DEC.

DEC also attends other events, for example, the Avalon International Airshow and the Chief of Army Land Forces Seminar, using these opportunities to raise awareness with those who may not have prior knowledge of export controls and may not understand the potential for them to apply to their business or activities.

A particular difficulty in raising awareness of the DTC Act is the lack of knowledge around the term ‘dual-use’ and the broad range of goods, technology and information that the term captures. Generally, if a person is aware of the DTC Act but does not associate their product or research with ‘defence’, that person will dismiss any application of the DTC Act. The university sector voiced concern in this regard because it is difficult for university administrators who manage export controls to ensure researchers consider DTC Act applicability and its implications for their research. One example cited was in the field of biofuel. Researchers working on developing fuel from algae ultimately developed a process to make high-grade fuel that could be used in jet engines. The fuel has application in commercial airlines, but it also has a possible parallel application in military aircraft, making it a potential dual-use item.<sup>38</sup>

Defence prime contractors raised concern about the less than optimal awareness of the DTC Act, and of export controls legislation more generally, among small and medium enterprises (SMEs) and the risks that this posed to the primes when using SMEs in their supply chains. Primes need the assurance that all elements of their supply chain are aware of the DTC Act (along with other export control requirements) and know when it applies and how to comply in order to reduce the risk of unauthorised transfer of technology.<sup>39</sup>

Industry stakeholders framed the issue in terms of there being no incentive for companies, in particular SMEs, to develop awareness about the DTC Act requirements because there are no visible consequences for non-compliance.<sup>40</sup> A comparison between the United States and Australia was made. The Bureau of Industry and Security (BIS), an agency of the US Department of Commerce, administers the Export Administration Regulations, which control the export and transfer of items on the US dual-use list—the Commerce Control List. BIS publishes the criminal convictions and the administrative measures taken in

---

38 Perth roundtable discussion, university session, 22 August 2018.

39 Melbourne roundtable discussion, industry session, 13 August 2018.

40 Melbourne roundtable discussion, industry session, 13 August 2018.

response to breaches of export control legislation.<sup>41</sup> Sanctions include administrative penalties, criminal fines, imprisonment and a provision that persons convicted are liable to be ineligible to apply for any export licence under the Export Administration Act for up to ten years from the date of conviction.

The United States applies a strong approach to manage compliance with export control laws. In 2017, the Department of Commerce negotiated with Chinese company ZTE a combined criminal and civil penalty of US\$1.19 billion after the company illegally shipped telecommunications equipment to Iran and North Korea.<sup>42</sup> It has been reported that, in 2013, Raytheon agreed to pay US\$8 million in civil penalties to resolve its violations of US export control laws.<sup>43</sup> In 2010, BAE Systems plead guilty to violations of the Arms Export Controls Act and International Traffic in Arms Regulations (ITAR) and was fined US\$400 million.<sup>44</sup> The consistent compliance and enforcement effort and application of penalties gets the message out and provides incentive for people to make themselves aware of export controls, discover whether the controls apply to them and implement compliance measures.<sup>45</sup> As a result of these compliance actions, the awareness of US export controls is widespread, both in the United States and internationally.

Stakeholders suggested that, in Australia, there is no visible action taken to address non-compliance and, therefore, there is no imperative to understand the DTC Act. Word of mouth has little effect, and lack of compliance action by the regulator means no real deterrent exists to discourage unintentional or deliberate non-compliance.<sup>46</sup> (A proposal to provide additional monitoring and investigation powers for Defence is discussed in Part 4 of this report.)

In the absence of any strong, public enforcement actions in Australia to provide an incentive for business to become aware of the DTC Act and comply with their obligations, it is essential for Defence to continue—and enhance—its awareness-raising program. In addition, it might be productive for Defence to consider partnering with other government or industry-specific initiatives, including the Centre for Defence Industry Capability, Austrade and industry peak bodies, to raise awareness.

### Recommendation 3

The Department of Defence (Defence) should allocate adequate resources to develop and deliver an effective program to ensure that key sectors, including university researchers and small and medium enterprises, are aware of their obligations under the *Defence Trade Controls Act 2012*. Defence should also explore partnering with other government or industry bodies to raise awareness.

41 US Department of Commerce, Bureau of Industry and Security, *Penalties* <https://www.bis.doc.gov/index.php/enforcement/oeep/penalties>.

42 US Department of Commerce, Secretary of Commerce Wilbur L. Ross, Jr. Announces \$1.19 Billion Penalty for Chinese Company's Export Violations to Iran and North Korea, 7 March 2017, <https://www.commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty>.

43 Reuters, *Raytheon agrees to pay \$8 million fine for export control violations*, 1 May 2013, <https://www.reuters.com/article/us-raytheon-exports/raytheon-agrees-to-pay-8-million-fine-for-export-control-violations-idUSBRE93T19720130430>.

44 US Department of Justice, *BAE Systems PLC pleads guilty and ordered to pay \$400 million criminal fine*, 1 March 2010, <https://www.justice.gov/opa/pr/bae-systems-plc-pleads-guilty-and-ordered-pay-400-million-criminal-fine>

45 Melbourne roundtable discussions, industry session, 13 August 2018.

46 Melbourne roundtable discussion, industry session, 13 August 2018.

## IS A MANDATORY COMPLIANCE STANDARD NEEDED?

Goal Professional Services (Goal) proposed that a compliance standard should be developed to underpin the DTC Act:

The Standard could then be called out in the Act, to be applied by all institutions handling international or Australian controlled technology. This standard will enable the Australian Government, or an external contractor, to implement a process for ensuring Australian Defence Exporters and Importers are fulfilling their obligations under the provisions of the Act.<sup>47</sup>

Queensland University of Technology supported the development of a robust Australian standard. It noted that such standards are informed by committees that comprise experts who would be able to formulate a workable standard, and noted that Australian standards can describe processes in detail and are reviewed regularly. The standard could also supply the mechanism for more explanatory definitions.<sup>48</sup>

Saab suggested a mandated compliance standard would give Saab ‘a clear picture of what standard it itself needs to meet and comfort that those it deals with (including in its supply chain) are “trustworthy” from a compliance perspective without (sometime costly and often resented) due diligence on Saab’s part’. Saab noted that it is not clear how such a standard would work in practice.<sup>49</sup>

Although there were no written submissions arguing against a compliance standard, there was very little other support in the roundtable discussions for a *mandatory* standard. It seems to the Review that the advantages proposed by advocates for a mandatory standard could equally be achieved by way of a voluntary standard. In such circumstances, it is not appropriate to recommend any additional regulatory requirements.

## COORDINATION ACROSS GOVERNMENT

Many stakeholders commented on the need to navigate across a wide range of Australian federal and state departments. The Export Council of Australia advised that it had received feedback that interactions with government regarding defence trade is very manual and administratively intensive for businesses particularly where multiple agencies are involved, such as when an exporter must obtain a sanctions permit from DFAT and an export declaration from the Department of Home Affairs.<sup>50</sup> The Export Council commented that as well as the government taking immediate steps to improve coordination, it would like to ‘see Defence trade controls eventually be included in the Single Window for Trade’.<sup>51</sup>

---

47 Goal Professional Services, submission 21, p. 2.

48 Queensland University of Technology, supplementary submission 11, p. 2.

49 Saab Australia Pty Ltd, submission 34, p. 2.

50 Export Council of Australia, submission 31, p. 2.

51 A ‘single window for trade’ can be defined as a system that allows traders to lodge information with a single body to fulfil all import- or export-related regulatory requirements; see [https://ec.europa.eu/taxation\\_customs/sites/taxation/files/resources/documents/customs/policy\\_issues/e-customs\\_initiative/ind\\_projects/swannexv.pdf](https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/policy_issues/e-customs_initiative/ind_projects/swannexv.pdf).

Saab expressed concern that there are multiple Acts of Parliament and multiple government agencies involved in regulating the movement of controlled military and dual-use goods across the Australian border. Saab commented in particular that it is 'illogical' to have part of Australia's DSGL-focused export control regime arising under the Customs Act and part under the DTC Act. This increases administrative overheads in that one application can result in two permit documents: one covering tangible export under the Customs Act and one covering intangible supply under the DTC Act. Saab requested that the Review consider whether a single permit could cover both tangible and intangible supply.<sup>52</sup>

It is outside the scope of this Review to examine this issue in detail or to make specific recommendations about coordination between different government programs, but the Review did observe significant uncertainty, confusion and frustration among stakeholders about this apparent lack of coordination. This Review observes that any progress towards integration or coordination between government agencies could yield significant benefits in terms of both compliance and the regulatory burden on the research and industry sectors.

---

52 Saab Australia Pty Ltd, submission 34, p. 2.

## PART 4: IS THE DTC ACT FIT FOR PURPOSE?

The DTC Act aimed to strengthen Australia's control over DSSL technology and goods by imposing controls on the intangible transfer of technology and arms brokering.<sup>53</sup> The Regulation Impact Statement underpinning the DTC Bill acknowledged that Australia's inability to regulate intangible technology transfers and arms brokering undermined the credibility of its export control regime.<sup>54</sup>

This Review was asked to consider whether the current DTC Act is fit for purpose—that is, whether it has effectively closed the gaps in Australia's defence exports regime by controlling the supply of DSSL technology, publication of DSSL technology and brokering of DSSL goods and technology. The Review was also required to deliver recommendations that will ensure the DTC Act is an effective component of Australia's export control regime that appropriately addresses current and future national security requirements.

### ENSURING CONTINUED ACCESS TO ALLIED TECHNOLOGY

The Defence submission to the Review noted that limited government oversight and control of the transfer of sensitive technology by Australians to foreign entities could have significant consequences for Australian defence capability, industry and universities. It suggested that potential consequences include:

Allied nations restricting Australian (government, industry and academics) access to defence and other security-related technology due to concerns it will not be afforded appropriate safeguards and protections. This could have significant consequences for ADF capability, inter-operability with partner forces and collaboration opportunities.<sup>55</sup>

The 2016 Defence White Paper states:

Access to the most advanced technology and equipment from the United States and maintaining interoperability with the United States is central to maintaining the [Australian Defence Force's] potency. Australia sources our most important combat capability from the United States, including fighter and transport aircraft, naval combat systems and helicopters. Around 60 per cent of our acquisition spending is on equipment from the United States. The cost to Australia of developing these high-end capabilities would be beyond Australia's capacity without the alliance.<sup>56</sup>

Defence advised the Review that the United States puts controls in place for the life of the technology, regardless of location and ownership. It also places restrictions on access by dual- and third-country nationals. Before the United States will permit a US company to send US-controlled technology to persons or entities in Australia, the receiver must agree to uphold certain conditions around who can access the technology. If the United States is not assured that recipients of the technology are appropriately safeguarding the technology, it may refuse access.

53 Explanatory memorandum, Defence Trade Controls Bill 2011, pp. 4–5, see [http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4700\\_ems\\_9e976e24-2fbc-48ae-ad31-dcf1d61d8eb7/upload\\_pdf/361899.pdf;fileType=application%2Fpdf](http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4700_ems_9e976e24-2fbc-48ae-ad31-dcf1d61d8eb7/upload_pdf/361899.pdf;fileType=application%2Fpdf).

54 Regulation Impact Statement, Defence Trade Controls Bill 2011; see [http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4700\\_ems\\_9e976e24-2fbc-48ae-ad31-dcf1d61d8eb7/upload\\_pdf/361899.pdf;fileType=application%2Fpdf](http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4700_ems_9e976e24-2fbc-48ae-ad31-dcf1d61d8eb7/upload_pdf/361899.pdf;fileType=application%2Fpdf).

55 Department of Defence, submission 46, p. 7.

56 2016 Defence White Paper, p. 122.

Mr Michael Shoebridge, Director of Defence and Strategy at the Australian Strategic Policy Institute, made a personal submission to the Review. Mr Shoebridge commented on the importance of protecting technology in the context of Australia's access to technology:

As it has in the past, future strategic and military advantage is likely to accrue to those who create and apply new technologies. The US and Australia have deep connections in scientific and academic research, and also in defence and intelligence applications of high technology.

Our current military advantage is based on technological and operational dominance, and our military and strategic weight is magnified by working with our international alliance and security partners.

Australian defence and intelligence capabilities contribute to our alliance. At the same time, Australia is critically dependent on the broad access it has to American systems, platforms and technologies to underpin our military and broader Defence organization. The dependence could not be replicated through other relationships. Seeking to be 'sovereign' in creation of indigenous capabilities as an alternative is likely not to be economically or demographically feasible.

...

Australia and the US share the most sensitive and advanced technologies we each have as part of the defence and intelligence relationships we have at the heart of our alliance. We protect such capabilities (like stealth platforms) once they exist with great care and effort so that our military advantages are not undercut.<sup>57</sup>

The Joint Strike Fighter (JSF) was given as an example of this collaboration and the requirement to protect the research and scientific advances that underpin the shared technology:

As an example, the JSF is the product of research and development that took place over the last 30 years. It is essential to protect the results of that research and development now that the JSF exists as a military capability.

To achieve this, Australia and the US between us will spend hundreds of millions of dollars securing the supply chains, maintenance facilities and classified data involved in building and operating the JSF over its life. The workforce to maintain and operate the aircraft will have high level security clearances, the hangars will be able to hold highly classified material and data and the electronic supply and maintenance systems will be cyber-hardened.

It is time we realized that the sources of our future strategic and military advantage—the front-end research and scientific advances that generate these future technologies—need equal protective effort.

We must act to prevent research relationships within each of our nation's academic and research institutions from enabling the militaries of other state actors who do not share our strategic interests.

The means for doing this exist in both our nations' policies and laws because of our commitment to international arms control and counter proliferation regimes.<sup>58</sup>

<sup>57</sup> Michael Shoebridge, submission 52, pp. 3–4.

<sup>58</sup> Michael Shoebridge, submission 52, pp. 4–5.

To ensure this continued access to international advanced military technology, Australian organisations, including Defence, the defence industry and universities must be able to demonstrate that appropriate controls and other mechanisms are in place to prevent illicit foreign access to this technology. The controls in the DTC Act are a crucial part of these arrangements, and any gaps in these controls could threaten Australia's access to this technology.

## A CHANGED NATIONAL SECURITY ENVIRONMENT

The Defence submission advised that in the last two years the national security environment has evolved and:

In order to effectively protect certain technology assessed as important to security and defence capability, the Australian Government needs the ability to regulate access to and transfer of military, dual-use and sensitive technology where the recipient's intentions may be prejudicial to the interests of Australia and its allies.<sup>59</sup>

Defence provided a classified annex that set out information about this changed national security environment. Although it is not possible to include details from the classified material in this public report, it is possible to report that the Review was provided with case studies where the current regime could not adequately protect Australia's national interests or where Australia's access to international technology could be threatened.

The Review was also provided with classified briefings from other Australian Government agencies, which tended to support the Defence submission.

The Australian Security Intelligence Organisation did not make a submission to this Review but did state in its 2017–17 annual report that 'in addition to traditional espionage efforts to penetrate government, foreign intelligence services are targeting a range of Australian interests, including clandestine acquisition of intellectual property, science and technology, and commercially sensitive information'.<sup>60</sup>

Mr Shoebridge also suggested that Australia's strategic environment had changed markedly since 2012, with direct implications for this legislation and the way in which it operates. He submitted that creating Australia's technological edge for our militaries and broader national security communities is a focus for our research community in partnership with government and the defence and technology sectors, and that this technological edge should be protected effectively in areas key to the military and broader national security community.<sup>61</sup>

---

<sup>59</sup> Department of Defence, submission 46, p. 7.

<sup>60</sup> Australian Security Intelligence Organisation, Annual Report 2016–17, p. 23.

<sup>61</sup> Michael Shoebridge, submission 52, pp. 3–4.

## ARE THERE GAPS IN THE CURRENT LEGISLATION?

Initial submissions from stakeholders indicated that most believed that the current level of controls in the DTC Act were appropriate. For example, the Australian Research Council advised:

It is the view of the ARC that these processes are working well and that the current controls of the DTC Act do not unnecessarily restrict research and international collaboration whilst ensuring current and future national security requirements.<sup>62</sup>

The Australian Industry Group said its members 'have expressed broad satisfaction with the operation of the Act'.<sup>63</sup> The Association of Australian Medical Research Institutes advised that 'the initial fears in the sector that this legislation would unduly inhibit researchers appear to have not materialised, and in large part this is because of the amendments made to the DTC Act before the offence provisions came into force'.<sup>64</sup>

In contrast, the Defence submission asserted that gaps exist in the current legislation, and it proposed options to strengthen regulation of the access to certain technology through the DTC Act in light of changes to the national security environment.<sup>65</sup> The apparent shortcomings in the DTC Act as identified by Defence are discussed in detail in the following sections.

### Locational limitations on supply too restrictive

The DTC Act does not require a permit if, at the point in time that supply occurs, both the supplier and receiver are located within Australia, both are located outside Australia, or the supplier is located outside Australia and the receiver is located within Australia.

Defence notes that:

foreign persons in Australia could obtain technology know-how which could be developed and used by their country of origin for security or defence purposes and, ultimately, such technology could be used in a manner prejudicial to Australia's interests. Australia must have a range of control measures to deal with the range of situations in which technology can be transferred.<sup>66</sup>

Classified case studies provided to the Review confirm that this lack of regulatory authority means that, in certain circumstances, the current legislation fails to provide a measure to restrict access to technology by foreign persons identified as having intentions hostile to Australia.

DFAT made a submission that supported this element of the Defence submission. It suggested that the Review should examine the desirability of strengthening the export control regime to include regulated military technological knowledge or know-how when it is transferred between Australian and foreign persons within and outside Australia.<sup>67</sup>

62 Australian Research Council, submission 36, p. 1.

63 Australian Industry Group, submission 49, p. 1.

64 Association of Australian Medical Research Institutes, submission 30, p. 1.

65 Department of Defence, submission 46, p. 1.

66 Department of Defence, submission 46, p. 7.

67 The Department of Foreign Affairs and Trade, submission 45, p. 2.

Thales Australia Limited (Thales) also noted that although the DTC Act addresses the issue of transfer or access to a DSGL technology between an Australian entity while in Australia and a foreign entity overseas, it does not address the 'needed controls if the foreign entity receives access to a DSGL technology while in Australia'. Thales also queried what happens when that same foreign entity leaves Australia and there are no assurances in place with respect to any unwanted third-party retransfer overseas. Thales noted that if an Australian entity, while overseas, supplies or provides access to DSGL technology to a foreign entity, this activity is also not captured under a permit requirement and asked what precludes an Australian entity from simply arranging an overseas trip and providing access instead of seeking an intangible supply permit.<sup>68</sup>

## **No controls for emerging and other technology not on the DSGL**

Defence raised concerns that technology assessed as significant to ensuring superior defence capability may not be captured by the DSGL, because the technology is emerging or does not meet the threshold to be controlled. In its submission, Defence proposed that the government should have the ability to control access to such technology by foreign entities when it is in the national interest. By way of example, Defence provided the following scenarios where dual-use technology is listed on the DSGL but is not controlled in these instances because it does not yet reach the required threshold:

### ***Technology for materials that can be used to make acoustic transducers for underwater detection:***

There are some cases where technology for the development of new materials used in underwater detection sensors has not required a permit, because the technology only relates to the raw material. To be controlled, the technology would need to be more specific and configured or specially designed for acoustic transducers (i.e. projectors, detectors). Advanced underwater sensing is an important capability, used by various sectors worldwide including militaries.

### ***Technology related to hypersonic research:***

A hypersonic air vehicle is capable of high speeds (around Mach 5 and above) and large ranges. Research in the field of hypersonics is dual-use i.e. it can be used to advance commercial avionic technology to decrease air travel times and increase fuel efficiency, however, it is also useful in a military context in the development of missiles. Often hypersonic data is not controlled because it can be considered as basic scientific research or below the DSGL technology threshold and is not directly applicable to military applications. However, Defence considers it important to have a mechanism to control this research due to the value the technology provides in the form of essential baseline understanding of fundamental hypersonic concepts and key aspects.

---

68 Thales Australia Limited, submission 40, p. 2.

The following is an example of technology that is not captured by the DSGL but where the research is currently developing the technology for a novel military end use:

***Technology that can contribute to 3D printing of energetic materials:***

Technology in additive manufacturing (or 3D printing) is rapidly advancing worldwide, including research in the area of 3D printing of polymeric compositions with inert fillers, with the ultimate aim of manufacturing rocket and artillery propellants. Often this technology is not controlled because it is not specific to energetic materials and export controls on 3D printing have not yet been internationally (or nationally) adopted. However, in some circumstances, it would be appropriate and necessary to have a mechanism to control the transfer of essential research in the developmental process for 3D printed propellants.

Mr Shoebridge also highlighted in his submission the need to regulate dual-use areas of research, of which some are subject to regulation now (quantum computing) and others currently are not (artificial intelligence and autonomy).<sup>69</sup>

The DFAT submission also suggested that the Review should examine the desirability of strengthening measures to regulate the export of defence/military technology that is not listed on the DSGL but is exported for a military end use.<sup>70</sup>

Murdoch University also raised concerns about items that are not listed on the DSGL that present potentially serious risks (for example, some influenza virus strains).<sup>71</sup> The Australian National University and DMTC noted that the DSGL has failed to keep up with technological change.<sup>72</sup>

## **Inadequate control of sensitive dual-use technology**

In the DTC Act, the controls on sensitive Part 2 (dual-use) DSGL technology are limited when compared with the controls on Part 1 (military) DSGL technology:

- The DTC Act regulates the publication of Part 1 (military) DSGL technology but does not regulate the publication of Part 2 (dual-use) DSGL technology.
- The DTC Act does not regulate the supply of DSGL Part 2 (dual-use) technology when the supply of the technology is preparatory to the publication of the DSGL technology. (The supply of Part 1 (military) DSGL technology is regulated when the supply of the technology is preparatory to the publication of the DSGL technology.)
- The DTC Act regulates brokering activities involving Part 1 (military) DSGL technology but does not regulate brokering activities involving Part 2 (dual-use) technology in the same way.

69 Michael Shoebridge, submission 52, p. 5.

70 The Department of Foreign Affairs and Trade, submission 45, p. 2.

71 Murdoch University, submission 22, p. 2.

72 Australian National University, submission 27, p. 1; DMTC, submission 20, p. 2.

Defence advised that this distinction arose as a way to reduce regulatory burden that was not commensurate with the security risk identified at the time of the amendment of the DTC Act in 2015, but advised that circumstances have since changed:

The distinction allows academics to submit papers relating to Part 2 technology for peer review or editing without the requirement to first obtain a permit. At the time, it was also assessed that the administrative burden for Government in regulating the publication of Part 2 DSGL technology and brokering activities involving Part 2 DSGL technology did not justify the benefit that might have been obtained.

Since that time, changes in the security environment necessitate stronger mechanisms to protect more sensitive dual-use Australian technology. These challenges have led Defence to reassess the situation. Part 2 of the DSGL contains technology that, while dual-use, is considered sensitive or very sensitive.<sup>73</sup>

Defence advised the Review that dual-use technology that is considered sensitive or very sensitive includes technology related to nuclear materials, chemicals, biological materials, and other technology related to weapons of mass destruction and their delivery systems.

## Defence recommendations to address the gaps in control

The Defence submission made three broad recommendations to address its concerns, specifically:

- the limitation of the supply provision at section 10 that specifies that it applies only when certain locational criteria are met at the time of supply
- the lack of control over the transfer of technology not captured by the DTC Act's existing provisions
- inadequate control of emerging and sensitive military and dual-use technology.

The Defence recommendations are:

1. That the Review consider measures to require a person to apply for a permit to supply or transfer DSGL or uncontrolled technology to foreign entities when the Australian Government notifies them [the person] that it has reason to believe the technology is significant to developing or maintaining national defence capability or could be used to prejudice the security, defence or international relations of Australia.
2. That the Review consider expanding the power [of the Minister under section 14 of the DTC Act] to prohibit the supply of technology to include both DSGL and uncontrolled technology.
3. That the Review consider expanding the DTC Act controls relating to the publication of DSGL technology, the supply of DSGL technology in preparation for publication, and the brokering of DSGL technology to regulate categories of sensitive technologies found in Part 2 of the DSGL.<sup>74</sup>

<sup>73</sup> Department of Defence, submission 46, p. 9.

<sup>74</sup> Department of Defence, submission 46, p. 9.

## Concerns about the Defence proposal

Following the publication of the Defence submission, a number of supplementary submissions were made raising concerns about the proposals set out in the Defence submission. There was a high level of consistency among the concerns raised in these submissions and in discussions at the roundtable meetings. The following general points are representative of these concerns.

### *Inadequate balance between national security and promoting research and trade*

Northrop Grumman Australia expressed concern that the Defence recommendations may not achieve the optimum balance between the necessary controls required to protect Australia's national security interests and its support for a commercially minded, collaborative and innovative environment in which Australia's defence industry can grow and be more competitive globally. Northrop Grumman suggested that the proposal may have the effect of limiting investment into critical research and innovation by industry and its research partners and requested that the Review consider the 'potential negative consequences for research, innovation and investment in, and by, the Australian defence industry which may result from implementing the level of controls suggested in the Defence submission'.<sup>75</sup>

Universities Australia summarised its understanding of the Defence proposal as 'suggesting that [Defence] be provided with the ability to control and prevent the export of any technology, at any time, at its sole discretion'. It advised that 'Universities Australia is deeply concerned about the impact the Defence proposals would have, if enacted. The proposals do not provide for an appropriate balance between security interests and a thriving research and development capability'. The Universities Australia submission states that the proposal could 'threaten investment in Australian research and development, making it more difficult to build new industries (including a defence industry), or achieve the ambitions of government initiatives such as the Global Innovation Strategy'. It questions whether the proposals are compatible with a number of Australian Government policies and suggests they may also be contrary to the ambitions of the broader National Innovation and Science Agenda.<sup>76</sup>

Australia's Chief Scientist noted that Australia is the net beneficiary of technology sharing. He questioned whether the risk of leakage and the difficulty of monitoring compliance justified stricter controls and more onerous regulation.<sup>77</sup>

### *Jeopardising international collaboration*

Numerous submissions and many participants at the roundtables emphasised the importance of international collaboration to modern research and stressed that international collaborative science programs commonly allow Australian researchers and innovators access to facilities and expertise not available in Australia, often for a fraction of their true cost. It was suggested that the Defence submission represented a substantial threat to such collaboration.

Universities Australia expressed concern that the proposal would damage Australia's competitive advantages by threatening international collaboration across a wide range of research fields and reducing the ability of Australia to compete for talented local and international researchers.<sup>78</sup>

<sup>75</sup> Northrop Grumman Australia, supplementary submission 18, pp. 1–2.

<sup>76</sup> Universities Australia, supplementary submission 13, pp. 1–3.

<sup>77</sup> Meeting with Dr Alan Finkel AO, 21 June 2018.

<sup>78</sup> Universities Australia, supplementary submission 13, pp. 1–3.

The Group of Eight supported this view. It submitted that Australia's national research capacity depends crucially on our researchers' ability to collaborate both domestically and internationally and that this collaboration is put at risk by Defence's proposal to introduce new measures to require researchers and others to apply for permits in additional, in fact unknown, circumstances—especially in relation to uncontrolled technology; to prohibit the supply of both DSGL and uncontrolled technology; and to restrict DSGL technology being published or being supplied in preparation for publication. The Group of Eight concluded that Defence's proposed measures have the potential to deter, if at the least only due to concerns over delays in processing times, Australian participation in certain areas of research.<sup>79</sup>

The Australian Academy of Science commented that it 'believes that further restrictions on Australian researchers' ability to engage in international research collaboration would be significantly detrimental to Australia's national interest; limiting our ability to benefit as a nation from the many international research collaborations and expertise on which a substantial proportion of our economy relies'.<sup>80</sup>

### *Increased uncertainty, complexity and compliance costs*

While acknowledging that the current system does not provide absolute certainty in that the DSGL can be amended and previously uncontrolled technology can become controlled, many stakeholders commented that the proposed changes would incur unacceptable additional uncertainty and lead to a reduction in investment in research. For example, Universities Australia wrote:

Should the supply of the products of research be controlled at the sole discretion of the regulator, it could considerably devalue the research. Even the uncertainty associated with the possibility of such control could make partners unwilling to invest in it—this would be a result contrary to the Australian government's policy of seeking to improve the commercialisation or translation of university research to end-users.

...

The proposals would make it difficult to achieve an innovative Australian defence industry. The possibility of a wide-ranging system of controlling any export could have the effect of significantly damaging the ability of both universities and those conducting commercial research endeavours to invest in the development of new technology. Without a clear understanding of the likelihood of whether an export will be controlled or not, there can be no understanding as to how a technology might be able to be developed or deployed, and hence the potential value of the technology is highly uncertain.<sup>81</sup>

The Australian Academy of Science advised that:

The Defence recommendations amount to the unilateral ability to prohibit, control or regulate any technology, irrespective of its status as a listed technology on the DSGL, and the ability to suppress publication of any given research activity. Such a regime would create enormous uncertainty, with no ability to determine whether a technology would be allowed to be developed, deployed, communicated or exported. This environment would not be conducive to investment in high quality research.<sup>82</sup>

<sup>79</sup> Group of Eight, supplementary submission 10, p. 2.

<sup>80</sup> Australian Academy of Science, supplementary submission 1, p. 2.

<sup>81</sup> Universities Australia, supplementary submission 13, pp. 3–4.

<sup>82</sup> Australian Academy of Science, supplementary submission 1, p. 3.

The Group of Eight commented:

The extension of controls to ‘uncontrolled’, unspecified technology would create significant uncertainty for researchers and those with whom they work, given the possibility that [Defence] may declare at any point in time that a technology is ‘emerging sensitive’ and subject to controls on transfers.<sup>83</sup>

Many stakeholders believed that this increase in uncertainty would lead to increased compliance costs. The Group of Eight commented:

Direct and indirect compliance costs, already considerable in our universities to deal with what is considered a tenable, reasonable situation under the current Act, would increase dramatically. The diversion of university resources and efforts to administration and to ensuring compliance would be unsustainable.<sup>84</sup>

The Australian Industry Group submitted that these concerns about uncertainty, compliance costs and complexity would also apply to industry and raised further concerns about the potential for inadvertent breaches.<sup>85</sup>

### ***Lack of scrutiny and transparency***

Stakeholders were concerned that the Defence proposal would provide the ability to restrict publication of even uncontrolled technology on the basis of information that is not open to public scrutiny.

Universities Australia considered that this would represent ‘a significant restriction of academic freedom and autonomy, as well as potentially undermining the effectiveness of the regulatory scheme’. It noted that, currently, the DSGL is public and is subject to parliamentary oversight:

The current system relies on the Defence and Strategic Goods List to ensure that researchers and other participants are able to reliably determine those technologies which may be subject to export controls. This list is publicly available and subject to Parliamentary oversight. This means the operation of the existing scheme is conducted upon known terms that support the rule of law and provide reasonable mechanisms for supervising the scheme’s operation. The proposals raised in the Defence submission seek to circumvent the DSGL, by allowing Defence to control supply and publication, regardless of whether Parliament has specifically allowed for it.

Such proposals, if implemented, would undermine confidence in the Defence Trade Controls regime, as well as the confidence of institutions supporting Australia’s national interests through innovation and technological development.<sup>86</sup>

---

83 Group of Eight, supplementary submission 10, p. 2.

84 Group of Eight, supplementary submission 10, p. 2.

85 Australian Industry Group, submission 49, p. 3.

86 Universities Australia, supplementary submission 13, pp. 4–5.

The Academy of Science also commented on the status of the DSGL:

Australia has an agreed and functional mechanism for identifying technologies with potential military applications which should be controlled: inclusion on the DSGL. As a legal instrument, the DSGL allows for transparency, consultation and Parliamentary oversight.<sup>87</sup>

### *Identifying foreign entities of concern*

Stakeholder submissions and the participants at the roundtable discussions suggested that the Defence proposal could require research institutions, including universities, and the defence industry to ascertain and keep registers of the nationalities of all researchers, including research students. Stakeholders raised the potentially devastating effects this might have on international collaboration and the financial impact on the university sector.

The Group of Eight questioned the advisability of ‘unmitigated extension of controls requiring the application of permits to supply or transfer DSGL or uncontrolled technology to foreign entities in Australia’. The Group of Eight suggested that ‘without careful and well-advised articulation of which foreign entities are of interest, a wide range of people would be in question—including foreign born Australian researchers, international PhD students in Australian universities, visiting Fellows or other research colleagues from overseas, multi-national companies with whom universities would otherwise be legitimately engaging’.<sup>88</sup>

Saab raised concerns about compliance with the proposed changes. It questioned how the proposed expansion of powers would operate to allow a company to identify those situations where a permit would be required to transfer to foreigners, including identification of the technology and the relevant foreign entities, and what type of due diligence would be required of companies. It was concerned to ensure that compliance would be achieved as simply, efficiently and cost effectively as possible.<sup>89</sup>

The issue of potential non-compliance with state and federal anti-discrimination laws and a requirement to obtain exemptions was raised in the roundtables. The general view was that these issues are not insurmountable but would add an extra layer of complexity and cost, particularly if such issues could not be resolved at the federal level.

### *Reduced cooperation with Defence*

A recurrent theme in submissions was the current excellent relationship that exists between research institutions, and industry with DEC. Defence also commented on the value of ongoing discussions with the sectors. Universities Australia stated that the Defence submission ‘undermines the effectiveness of the Defence Export Controls regime by reducing the trust and cooperation between Defence and the research sector that is essential to the success of the scheme’. It suggested that the proposals ‘run the risk of damaging the cooperative and constructive approach that the university sector has taken in engaging with the DTC Act’.<sup>90</sup> Other participants at the roundtables suggested that if the controls were broadened in the manner proposed by Defence, future researchers could be more reluctant to discuss their technology or seek a Defence assessment of their research technology.

87 Australian Academy of Science, supplementary submission 1, p. 2.

88 Group of Eight, supplementary submission 10, p. 2.

89 Saab Australia Pty Ltd, supplementary submission 19, pp. 6–7.

90 Universities Australia, supplementary submission 13, pp. 1–3.

## HOW SHOULD THE GAPS BE ADDRESSED?

### Balancing national security with trade, research and international collaboration

Although the Review was persuaded that the gaps in the legislation as identified by Defence need to be addressed in order to achieve the aims of the legislation in a changed national security environment, the Review is also mindful of the obligation to ensure that any amendments do not unnecessarily restrict trade, research and international collaboration.

The Review does not support the broad approach implied by the recommendations in the Defence submission.

### Consultation with affected groups

Defence and other stakeholders acknowledged that any amendment to the DTC Act must 'be developed in consultation with affected groups and in the spirit of working together to ensure Australia's interests are protected'.<sup>91</sup> Universities Australia said that it would welcome such engagements and that it is committed to ensuring that the regulation of research is effective and efficient.<sup>92</sup>

The Australian Industry Group commented that the success of the DTC Amendment Act and its implementation demonstrates the importance of early and deep engagement with the industry and academic stakeholder community in the development of this sensitive area of policy and legislation. It suggested that 'successful implementation of further protections will only occur if the stakeholder community understands (broadly) the basis of the changes and the new policy and legislation amendments and agrees that they are workable in partnership with Defence'.<sup>93</sup>

This Review supports the proposition that direct and ongoing consultation is required between Defence and stakeholders to develop a policy proposal that takes a proportionate approach to address the current gaps in the legislation but also addresses the serious and legitimate concerns of industry, research bodies and universities.

### Applying a targeted approach

The control of the transfer of technology should be proportionate, targeted and based on risk. Such an approach would have the benefit of focusing effort and resources on protecting technology that would cause the most damage should it be obtained by foreign entities that may use it against Australian interests.

Consistent with the existing approach, the risk should be based on consideration of the technology being supplied, the end user, and the end use. Providing clearer guidance around what is to be regulated and why, may address most concerns within the defence industry and universities and hence focus effort and debate around the actual national security interests involved.<sup>94</sup>

---

91 Department of Defence, submission 46, p. 1.

92 Universities Australia, supplementary submission 13, p. 5.

93 Australian Industry Group, submission 49, p. 2.

94 Michael Shoebridge, submission 52, p. 1.

## Controls on technology not on the DSGL

According to its submission, Defence seeks to control the transfer of uncontrolled technology where it has reason to believe the technology is significant to developing or maintaining national defence capability or could be used to prejudice the security, defence or international relations of Australia.

Although inclusion of the particular technology on the DSGL would ensure transparency, scrutiny and reasonable certainty, the DSGL is a legislative instrument that incorporates the goods and technology agreed, by consensus, as requiring control. Securing additions to control lists is a lengthy process because of the number of member countries and the requirement for consensus. Translating these updates into the DSGL to then be approved by government and parliament as a disallowable legislative instrument is a further time-consuming process. As a result, the DSGL may never be reflective of the most current state of technology.

Further, adding technology to the DSGL would mean that it would be controlled by all legislation that is underpinned by the DSGL. That is, all controls in the DTC Act and the Customs PE Regulations would apply to technology—that would otherwise be uncontrolled—if it were included on the DSGL. Sanctions legislation administered by DFAT also relies to an extent on the DSGL for its determination of ‘arms and related materiel’. Additionally, technology may be named on the DSGL, but the technology of concern that is to be transferred may not meet the threshold or specifications in the DSGL for it to be controlled.

The Review understands that it is not the intent of the risk-targeted approach proposed by Defence to regulate the transfer of all DSGL technology to foreign entities, and in its submission Defence dismisses this option of ‘regulating transfers of all DSGL technology to foreign entities [because it] would be administratively burdensome for both the regulator and applicants, and it would not necessarily be driven by risk or capture all technology assessed as requiring control, such as emerging and developing defence technology’.<sup>95</sup>

A risk-based approach would ensure that controls apply only to those technologies that present the greatest risk to defence capability if obtained by foreign entities located within or outside Australia with interests prejudicial to Australia.

Mr Shoebridge identifies as emerging technologies ‘notably technologies of the near and medium term like telecommunications and network technologies, artificial intelligence, quantum computing, autonomy, biotechnology, hypersonics, directed energy, nanotechnology and new materials’.<sup>96</sup>

Queensland University of Technology commented on the issue of technological advances moving fast and suggested that a panel of experts with appropriate technical and scientific expertise was required to consult in consideration of the DSGL.<sup>97</sup>

It is possible that the relevant currently uncontrolled technology that could require control would similarly be best identified in a collaborative approach by a group of experts from Defence and other relevant stakeholders. It should also be possible to provide a certain level of scrutiny and transparency if the decision that the supply of a particular uncontrolled technology should be subject to control were made by the Minister.

---

<sup>95</sup> Department of Defence, submission 46, p. 7.

<sup>96</sup> Michael Shoebridge, submission 52, p. 3.

<sup>97</sup> Queensland University of Technology, submission 33, p. 2.

## Identification of sensitive dual-use technology

Defence advised the Review that a technology is considered sensitive if it is acquired or exploited and could degrade mission effectiveness, shorten life of a system in terms of combat effectiveness, reduce Australian Defence Force (ADF) technological advantage, or has application in a weapon of mass destruction or a system to deliver a weapon of mass destruction.<sup>98</sup>

Mr Shoebridge noted the difficulty of identifying sensitive dual-use technology and proposed that the research sector should also be engaged in the identification of the likely end users of their research:

as the military uses, while critical, are not the dominant ones (self-driving technology is suited to both cars and tanks, for example), so regulation will likely need to focus on the proposed end user nation and involve risk-based assessments made together with the research community and our tech sectors. Our research sector can help by working to understand both their research partners and the actual likely end users of their work.<sup>99</sup>

Again, it is likely that a collaborative approach with the research sector will be required to identify the sensitive technologies that require control.

It should also be possible to provide a certain level of scrutiny and transparency if the decision about what type of dual-use technology was determined to be sensitive and could be subject to control was made by the Minister.

## Broadened ministerial prohibition power

While sections 14, 14B and 15A of the DTC Act give the Minister a non-delegable power to give a notice prohibiting certain activities relating to DSGL goods and technology if the activities would prejudice the security, defence or international relations of Australia, these prohibition powers are not available in respect of non-DSGL technology. The Defence recommendation would extend these powers to include the prohibition of the supply of uncontrolled technology.

There are already significant safeguards in the exercise of these powers. They need to be exercised by the Minister personally. A person who is aggrieved may seek review of these decisions by the Administrative Appeals Tribunal as well as under the *Administrative Decisions (Judicial Review) Act 1977*. There is no statutory reporting requirement for the exercise of this power, but Defence does publish on its website the number of prohibition notices issued under the DTC Act.<sup>100</sup> (No prohibition notices were issued in the 2017–18 financial year.)

While this Review cannot support this Defence recommendation in its current broad form, the Review does support consideration of the extension of this prohibition power subject to the development of a satisfactory means of specifying the uncontrolled technology, the supply of which would be prohibited.

<sup>98</sup> Advice from DEC technical assessors, September 2018.

<sup>99</sup> Michael Shoebridge, submission 52, p. 5.

<sup>100</sup> Department of Defence, Defence Export Controls, *DEC Statistics*, <http://www.defence.gov.au/ExportControls/statistics.asp>.

## Removing the locational limitation on supply

Defence identified the inability to control the transfer of technology to a foreign entity in Australia as a gap in the legislation that needed to be remedied; however, regulating the transfer of *all* DSGT technology to foreign entities, regardless of location at the time of supply, would be administratively burdensome for both the regulator and the applicants, and it would not necessarily be driven by risk.

If a risk-based approach were taken, entities of concern would be those individuals identified by Defence as being likely to transfer a particular technology to a particular end user to be used in a particular manner that would involve a high risk to security, defence capabilities or Australia's international relations. Such entities could include, for example, a person acting for, or on behalf of, a foreign power that has intentions prejudicial to the interests of Australia and its allies.

This proposal attracted a high level of stakeholder concern and, according to submissions to the Review, has the potential to have a significant economic and reputational impact on research institutions, cause detriment to individual researchers, and jeopardise the relationships between Australian entities and foreign counterparts.

The Defence proposal relies on a person receiving notification that they are required to obtain a permit rather than a person identifying the requirement themselves. It would be expected that a decision to notify a person that a permit is required would be preceded by discussion and consultation, including providing reasons for the notification where possible, and that receipt of such a notice would not be unexpected. Given the sensitivity of the decision, it could also be appropriate for it to be made at a ministerial level. It is also expected that such a decision would be reviewable.

## ENSURING A PROPORTIONATE RISK-BASED APPROACH

While it would be premature for the Review to formulate any prescriptive recommendations for legislative amendments, it is appropriate to articulate principles that could guide such changes.

### Recommendation 4

The Department of Defence should work with stakeholders to develop a practical legislative proposal to address the following gaps in the *Defence Trade Controls Act 2012* (DTC Act):

- the limitation of the supply provision at section 10 that specifies that it applies only when certain locational criteria are met at the time of supply
- the lack of control over the transfer of technology not captured by the DTC Act's existing provisions but which, if transferred to foreign entities with interests contrary to Australia's, could prejudice Australia's security, defence and international relations
- the inadequate control of emerging and sensitive military and dual-use technology.

To ensure that any amendment does not unnecessarily restrict trade, research and international collaboration, the legislative proposal should:

- ensure all decisions are targeted and based on risk-related consideration of the technology being supplied, the end user and the end use
- contain measures to ensure transparency and scrutiny of decisions
- limit additional uncertainty, complexity and risk of inadvertent breaches
- minimise any increased compliance costs.

# BROKERING OF CONTROLLED GOODS AND TECHNOLOGY

## Background

The DTC Act introduced controls on ‘brokering’ activities under Division 2 of the DTC Act. A broker undertakes a regulated activity that involves arranging for another person to supply and transfer DSGL goods or technology between two places located outside Australia. ‘Arranging for another person to supply DSGL goods or technology’ is defined in section 5A of the DTC Act as acting as an agent of a person, or acting as an intermediary between two or more persons in relation to the supply. For the activity to be regulated, the intermediary or agent must receive money or a non-cash benefit, or advance their political, religious or ideological cause, in return for arranging the supply.

The current definition of brokering in the DTC Act focuses on the relationships between parties rather than on the activities (facilitating arms sales or movements) that constitute brokering. The DTC Act controls only those instances where a person or entity acts as an agent or intermediary for the supply of military goods, or dual-use goods with a WMD or military end use. The terms ‘agent’ and ‘intermediary’ could indicate that the supplier and recipient must both be aware and intend to act as a supplier (supplying to the recipient) or as the recipient (receiving from the supplier) in the brokering arrangement.

## Submissions

Defence advised that the definition of brokering in the DTC Act does not clearly capture the following transactions:

- where Australian entities create and operate subsidiaries from a third country in order to avoid compliance with Australian export controls
- where a vendor organises for the purchased items to be sourced from overseas to fill its contracts.

In its submission, Defence proposed that the definition of the term ‘brokering’ be amended to remove the requirement for the broker to be acting as an agent or intermediary.<sup>101</sup>

Saab expressed concern that situations that Saab had previously determined were not brokering, including through discussion with DEC, would become brokering under the Defence proposal, and to understand how the proposed expansion of controls would operate to allow an entity to identify situations where a permit to broker is required, obtain the permit and keep appropriate records of the brokering. Saab also commented that the proposed amendment would increase administrative and cost burdens, which would lessen Australian exporters’ competitiveness on the international market.<sup>102</sup>

## Discussion

The Review considered a scenario involving an Australian company supplying a foreign defence force (in country A) with DSGL controlled goods from a foreign supplier (in country B). The Australian company has two separate agreements: one with the foreign defence force, and a separate one with the foreign supplier. It could be argued that in such arrangements the company might not be acting as an agent or intermediary between the two parties, and the brokering provisions of the DTC Act would be avoided. This is not consistent with the intent of the DTC Act.

<sup>101</sup> Department of Defence, submission 46, p. 10.

<sup>102</sup> Saab Australia Pty Ltd, supplementary submission 19, p. 9.

The Review agrees that the definition of 'brokering' should be amended to remove this doubt. The Review is also mindful of the need for consultation to ensure that companies are aware of how the amended provision would apply and to enable them to ensure compliance.

## Recommendation 5

The Government should consider amending the definition of 'arranging for persons to supply goods or DSSL technology' (that is, 'brokering') in the *Defence Trade Controls Act 2012* to ensure that the provision clearly reflects the objectives of the Act. Any amendment to the legislation should be communicated effectively to affected entities.

## MONITORING AND INVESTIGATION POWERS

### Background

The Australian Border Force is responsible for enforcing regulations that control the export of DSSL goods. Goods leave the country via air and seaports, where Australian Border Force officers can inspect goods to ensure their export is not in violation of the Customs (PE) Regulations. The Customs enforcement framework does not enforce regulation of the intangible transfer of technology.

Administrative investigations and inspections by regulators have a significant part to play in monitoring transfers of technology. The DTC Act provides information-gathering powers to the Secretary of Defence (or their delegate) to allow the Secretary to obtain information from a person if the information is relevant to the operation of the DTC Act. The information-gathering powers allow the Secretary or a delegate to require the production of specific information or documents.

Part 4 of the DTC Act sets out monitoring powers in relation to the Australia–US Defense Trade Cooperation Treaty. In summary, an authorised officer may enter certain premises at any reasonable time of day for the purpose of ascertaining whether the person has complied with Part 3 (Defense Trade Cooperation Treaty) or Part 6 (Record-Keeping) of the DTC Act or a condition of the section 27 approval (that is, approval to be a member of the Treaty's Australian Community). The authorised officer must give the person at least 24 hours' notice of the officer's intention to enter the premises. An authorised officer who enters premises may exercise specified monitoring powers. These powers only apply to the Australia–US Defense Trade Cooperation Treaty parts of the DTC Act and are available only in relation to a person who has been approved as a member of the Australian community.

## Submissions

Defence submitted that it does not currently have general powers to comprehensively gather information to monitor compliance, or to effectively investigate suspected non-compliance to determine whether cases should be referred to the Australian Federal Police or administrative compliance action should be taken. In its submission, Defence proposed an extension of the application of the DTC Act's Part 4 monitoring powers to Part 2 of the DTC Act.

In supplementary submissions, other stakeholders expressed concerns about this Defence proposal. The University of Adelaide advised that the proposed extension would result in 'a significant administrative and financial burden on the University and research sector'.<sup>103</sup> Universities Australia and the Australian Academy of Science commented that the Defence proposal meant that Defence would be given 'warrantless search and seizure powers' to effect compliance with its expanded remit.<sup>104</sup>

## Discussion

The *Regulatory Powers (Standard Provisions) Act 2014* (RP Act) creates a framework for the provision of:

- monitoring powers, which can be used to monitor compliance with provisions of an Act and to monitor whether information given to the Commonwealth is correct (Part 2)
- investigation powers, which can be used to gather material that relates to the contravention of an offence or civil penalty provision (Part 3).

When exercising either monitoring or investigation powers, the RP Act requires that an authorised person can enter a premise only if the occupier has consented to the entry or the entry is made under the relevant warrant.

The standard provisions have now been triggered by a range of Commonwealth regulatory regimes. The Attorney-General's Department advises that '[p]roposals that seek to establish or amend frameworks that provide for regulatory powers should trigger the standard provisions of the RP Act, unless there are compelling policy reasons to the contrary.'<sup>105</sup>

The Review considers that it would be appropriate for this suite of powers, available only by consent or under a warrant, to be considered for use by Defence in monitoring and investigating compliance with the DTC Act. Additional specialised and properly trained staff should be made available to Defence for this purpose. The introduction of these powers should not significantly increase the regulatory burden on the users of the system. The proposal should not require additional compliance activities or record keeping by institutions; the monitoring powers would be available to ensure compliance with any requirement already set out by law or as a condition of a permit.

### Recommendation 6

The Government should consider triggering the general monitoring and investigation powers set out in *Regulatory Powers (Standard Provisions) Act 2014* for use by the Department of Defence to monitor and investigate compliance with the *Defence Trade Controls Act 2012* and ensure that additional properly trained staff are allocated to exercise these powers.

<sup>103</sup> University of Adelaide, supplementary submission 4, p. 1.

<sup>104</sup> Universities Australia, supplementary submission 13, p. 3; Australian Academy of Science, supplementary submission 1, p. 2.

<sup>105</sup> Attorney-General's Department, *Regulatory Powers*, <https://www.ag.gov.au/LegalSystem/Pages/Regulatory-powers.aspx>.

## FUNCTIONALLY EQUIVALENT METHODS OF THE SUPPLY OF TECHNOLOGY

While expressing broad satisfaction with the current operation of the DTC Act, a number of submissions pointed to some other apparent deficiencies in the current legislation:

- Northrop Grumman noted that the inconsistent application of permit requirements—in relation to supply of the identical DSGL controlled technology to the same person outside Australia—can lead to confusion and be difficult to manage. For example, no permit is required if an individual saves DSGL controlled technology on their email account while in Australia and then accesses that technology while in another country, and no permit is required if that same individual then passes that technology to another person while outside Australia, but a permit is required for that same individual to email the same export controlled technology to the same person outside Australia.<sup>106</sup>
- Queensland University of Technology also pointed to an apparent inconsistency or loophole whereby there are no controls over the supply of technology where an Australian researcher is overseas and uses a virtual private network to access a controlled dual-use technology and distribute it to a third party. This seems to be equivalent to taking a USB overseas, or sending the controlled technology via email—both of which require a permit.<sup>107</sup>
- University of Wollongong also pointed to the inconsistency in relation to DSGL technology generated in Australia by ‘an international student or researcher as part of a collaborative agreement or research project, who subsequently owns the IP and upon return to their country of origin would be exporting this technology and potentially disseminating it either via the cloud, USB or some other uncontrolled method’. University of Wollongong also noted that oral dissemination of DSGL technology at an international conference is covered by the DTC Act, but the publication of this material in a set of conference papers or an electronic submission of a presentation for uploading online by the conference organisers do not seem to be covered.<sup>108</sup>
- Murdoch University suggested an inconsistency whereby a permit might not be required for a research talk, but a similar PowerPoint presentation might require a permit.<sup>109</sup>

These submissions highlight the issue of the difficulty of controlling functionally equivalent methods of supplying or publishing technology. Some of these outcomes are counterintuitive and causing confusion among users. It is not possible to say with any certainty whether these loopholes are being exploited and undermining the objective of the DTC Act, but it would be prudent for the government to consider these concerns and whether the DTC Act requires amendment to ensure that appropriate controls apply that are independent of the technical method used to supply or publish the technology, especially as these methods continue to develop and change.

### Recommendation 7

The Government should consider amending the *Defence Trade Controls Act 2012* to ensure that the Act's objectives are achieved by ensuring that the regulation is independent of the technical method used to supply or publish technology.

<sup>106</sup> Northrop Grumman Australia, submission 43, p. 1.

<sup>107</sup> Queensland University of Technology, submission 33, p. 2.

<sup>108</sup> University of Wollongong, submission 42, p. 2.

<sup>109</sup> Murdoch University, submission 22, p. 2.

THIS PAGE IS INTENTIONALLY BLANK

# PART 5: POSSIBLE REGULATORY OVERREACH

## THE ‘BASIC SCIENTIFIC RESEARCH’ EXEMPTION

Submissions from the research and university sectors suggested that the ‘basic scientific research’ exemption in the DSGL is not aligned with the export controls of like-minded partners, in particular the United States but also the United Kingdom.<sup>110</sup> Submissions suggested that Australia’s ‘basic scientific research’ exemption, which does not include research undertaken with a specific aim, is overly restrictive because the vast majority of research, even at the basic and theoretical levels, is performed with the broad objective of a specific application.<sup>111</sup> The consensus was that the exemption applied by Australia disadvantaged Australian researchers compared with their overseas colleagues, particularly in the United States where, according to the submissions, a ‘fundamental research exemption’ applies to export controls.

The DSGL exempts technology that is ‘basic scientific research’ and defines the term as:

experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.<sup>112</sup>

The submissions that raised the ‘basic scientific research’ exemption as too restrictive argued that the United States has added a universally applicable ‘fundamental research’ exemption to its export controls. This statement about the US system does not seem to be entirely accurate. The US ‘fundamental research’ exemption included in the Export Administration Regulations (EAR)<sup>113</sup> may apply to technology and research included on the Commerce Control List (CCL)—the US dual-use list—but its application is caveated and not universally applicable.<sup>114</sup> In addition, the ITAR, which regulates technology on the US Munitions List (USML) does not have a fundamental research exemption at all; rather, the definition forms part of the ‘public domain’ exemption and only applies if the information is already published and generally accessible to the public.<sup>115</sup> The EAR provides that CCL technology or software that arises during, or results from, fundamental research and is intended to be published is not subject to EAR controls.<sup>116</sup> The EAR definition of ‘fundamental research’ is:

research in science, engineering or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which researchers have not accepted restrictions for proprietary or national security reasons.<sup>117</sup>

110 See, for example, University of Melbourne, submission 24, pp. 1–2; Australian National University, submission 27, pp. 1–2.

111 See, for example, University of Melbourne, submission 24, pp. 1–2; Stephen Hyde, submission 16, pp. 1–2.

112 Defence and Strategic Goods List, Division 4, <https://www.legislation.gov.au/Details/F2016C00970>.

113 Section 734.8(c) Export Administration Regulations, <https://www.bis.doc.gov/index.php/documents/regulation-docs/412-part-734-scope-of-the-export-administration-regulations/file>.

114 Bureau of Industry and Security, *Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions*, <https://www.bis.doc.gov/index.php/forms-documents/compliance-training/export-administration-regulations-training/1554-ear-definitions-faq/file>.

115 Section 120.11 International Traffic in Arms Regulations, [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_111](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_111).

116 Section 734.8(a) of the Export Administration Regulations <https://www.bis.doc.gov/index.php/documents/regulation-docs/412-part-734-scope-of-the-export-administration-regulations/file>.

117 Section 734.8(c) of the Export Administration Regulations, <https://www.bis.doc.gov/index.php/documents/regulation-docs/412-part-734-scope-of-the-export-administration-regulations/file>.

Determining whether research falls within the definition of ‘fundamental research’ in the EAR is complex, as illustrated by the advice published by the Bureau of Industry Security, the agency in the US Department of Commerce that administers the EAR.<sup>118</sup> This advice makes it clear that not all research that satisfies the definition of ‘fundamental research’ is exempt in every circumstance. The restrictions on the application of the fundamental research exception are complex and include:

- proprietary research
- research methods or outcomes of government-funded research that have been specifically restricted from publication
- any research methods or outcomes that have been communicated in violation of any condition that may exist in a funding instrument that requires prepublication security review of the research communication
- research methods or outcomes that a researcher voluntarily decides should not be communicated widely because of security concerns and therefore self-redacts from publication.

The ITAR exempts technology captured by the USML from control if it falls within the definition of ‘public domain’. The ‘public domain’ definition in the ITAR includes, among other things, information that is published and generally accessible or available to the public:

through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

- (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or
- (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.<sup>119</sup>

Publicly available advice from the Directorate of Defense Trade Controls, the agency that administers the ITAR in the US Department of State, is that fundamental research is predominately controlled by the ITAR. The only part of fundamental research that is not controlled by the ITAR is the published information that meets the definition of ‘public domain’ at section 120.11.<sup>120</sup>

In contrast, Australia has a single control list, the DSGL, which incorporates both military and dual-use goods and technology and applies the ‘basic scientific research’ without restriction; any technology or research that falls within the definition is exempt from control. However, if technology does not fall within the ‘basic scientific research’ exemption, it still may not be controlled because it is not ‘required’ for the ‘development’ ‘use’ or ‘production’ of an item— the threshold for control in the DSGL.

---

118 Bureau of Industry and Security, *Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions*, pp. 4–9; see <https://www.bis.doc.gov/index.php/forms-documents/compliance-training/export-administration-regulations-training/1554-ear-definitions-faq/file>.

119 Section 120.11 of the International Traffic in Arms Regulations, [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_111](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_111).

120 Tony Dearth, Chief, Space & Missile Technology Division, Department of State/DDTC Licensing, *Fundamental Research According to the ITAR*, <https://www.colorado.edu/researchinnovation/sites/default/files/attached-files/FundamentalResearchandSpaceInstrumentation.pdf>.

The definition of ‘basic scientific research’ in the DSGL has been agreed by the multilateral export control regimes and adopted by most member countries, for example, the United Kingdom. In the United Kingdom, as in Australia, controls on technology transfer do not apply to ‘basic scientific research’.<sup>121</sup> In addition to the exemption for basic scientific research, the DSGL also exempts from control any information in the public domain and the minimum information necessary for a patent application.

The Review finds that a direct comparison of definitions of exemptions used in the US and Australian export control systems was not possible or useful because of the inherent differences in the systems and the complexity of the US system.

During the consultation process, the Review explicitly sought from stakeholders examples of when the ‘basic scientific research’ exemption to Australian export controls had resulted in an activity being controlled in Australia that was not controlled in the United States. Although a hypothetical case study was provided, no actual instances of this occurring were brought to the attention of the Review.

While the Review accepts that the exemptions in Australia may not align exactly with those in the United States, it was not persuaded that a case to amend the ‘basic scientific research’ exemption has been made out at this stage.

## **IS THE CURRENT REGULATION OF CRYPTOGRAPHIC RESEARCH APPROPRIATE?**

### **Background**

All cryptographic items subject to export control are listed in Category 5, Part 2 of the DSGL. The goods in this section include cryptographic radios and other information security devices; software used in such goods; and technology (technical data) required to design, produce and use these goods. This part of the DSGL is structured as a negative list with exemptions, which means it is likely to capture a broader range of controlled goods, software and technology in comparison to the rest of the DSGL.<sup>122</sup>

In response to concerns raised about the implementation of the DTC Act in the area of cryptographic research, Defence commenced a trial of two-step permits in early 2017 for information security and cryptography research.

The first permit is a broad permit to enable the early stages of collaboration and research to proceed with a minimal level of regulation and provide a trigger (via a notification from the researcher) for DEC to assess if a second permit is required. The second permit, which should only be required in limited circumstances, will enable more sensitive projects and collaborations to proceed under a tailored permit that will be crafted to address the identified level of risk. The aim of the two-step permit is to achieve a balance between national security interests and the need for the free flow of information for research purposes in the initial stages of a research project.<sup>123</sup>

---

121 Department for International Trade, *UK Strategic Export Control Lists*, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/685044/controllist20180305.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685044/controllist20180305.pdf).

122 Department of Defence, Defence Export Controls, *Trial of 2-step permits for Information Security and Cryptography Research will begin soon*, <http://www.defence.gov.au/ExportControls/CryptoPermitTrial.asp>.

123 Department of Defence, Defence Export Controls, *Trial of 2-step permits for Information Security and Cryptography Research will begin soon*, <http://www.defence.gov.au/ExportControls/CryptoPermitTrial.asp>.

## Submissions

The Australian Universities Cryptography Researchers submission addressed what they term ‘the unintended consequences’ of the DTC Act for Australian cryptography research. Their submission suggested that the regulation of cryptography was counterproductive and advised that problems arose for researchers when communicating internationally, but before publication:

Cryptography is the mathematical science of controlling the flow of information. It is not a weapon and cannot be used as a weapon. It does not belong in the Wassenaar arrangement and should be removed. Unfortunately, the arrangement does not allow Australia simply to remove parts of the treaty from our Defence [and] Strategic Goods List.

Encryption is one of the foundations of cybersecurity. Australia’s shortage of skills in this area has already been described as a threat to our future national security. Australian businesses are also clamouring for graduates with these skills as the need for in-house cybersecurity expertise becomes crucial: e.g. Banks, telcos, and the public sector. Restrictions on research and teaching of fundamental skills and new advances in cybersecurity constrict the pipeline for such graduates. This makes us less secure and makes our industries vulnerable to malicious online actors. Many Australian cryptographers work overseas, and most Australian universities struggle to find people with adequate technical cybersecurity skills. The DTCA’s penalties and restrictions on the communication of cryptography research indirectly jeopardise our future national security.

It is not true that the DTCA’s restrictions on communication about cryptography bring us into line with like-minded countries. Most other Wassenaar participants are liberal democracies with explicit constitutional protections of free speech. Though some have restrictions on the books, there is substantial precedent for regarding them as inconsistent with the constitutional protection of free communication. For example, in the US case of *Bernstein vs the Department of Justice*, the US 9th circuit court of appeal found that the export of source code for encryption was protected by the First Amendment. EU directives have also emphasised the importance of encryption for protecting the right to free communication. Australia was particularly singled out by the International Association for Cryptologic Research for subjecting ‘many ordinary teaching and research activities to unclear, potentially severe, export controls.’<sup>124</sup>

Dr Vanessa Teague gave as an example of a technique that falls foul of the DSGL a new technique for counting encrypted preferential votes in an election without disclosing individual votes. The technique involves a key length in excess of that prescribed in the DSGL and thus a permit would be required.<sup>125</sup>

---

<sup>124</sup> Australian Universities Cryptography Researchers, submission 14, p. 1.

<sup>125</sup> Dr Vanessa Teague, by telephone, 9 August 2018.

The Australian Universities Cryptography Researchers were involved in the two-step permit trial:

Some of us were included on the ICT working group established by the strengthened export controls steering group, which included Defence Export Controls (DEC), who have been as accommodating and flexible as they can be in the circumstances. We've worked together on drafting a significantly lighter and broader permit process, which will allow academics a broad permit for international cryptography research, with a requirement to notify DEC but without the need to get permission before commencing work ...

In the absence of legislative change ... the broader permits are a reasonable amelioration, though they still leave cryptography researchers at risk if there is a change of policy.<sup>126</sup>

The University of Melbourne described their experience with the two-step trial permits as 'very positive to date' and said that the broader permits 'serve to reasonably ameliorate the tensions experienced by university researchers'.<sup>127</sup>

## Discussion

Comments at the roundtables supported the proposition that collaboration in cryptographic research of the type that did require permits in Australia did not require permits in other countries, including the United States.

It was not possible for the Review to verify this anecdotal evidence by examining the US legislation because of the complexity of, and interaction between, the various regulations and arrangements (including exemptions) that are in place between the US Government and various US research institutions.

Similarly, although the Review accepts the proposition that Australian cryptographic researchers should be subject to similar, but not more severe, regulatory constraints as their counterparts in the United States, the Review cannot make any specific recommendation to amend the DTC Act to achieve this because of the dependence on the DSGL (a multilateral instrument). This may, in fact, not be a legislative issue but rather one of the interpretation of DSGL thresholds.

While noting a preference for a blanket exemption, stakeholders have expressed clear support for the approach taken in the Defence two-step cryptography trial. It would now seem timely for Defence to conduct a formal evaluation of the trial with stakeholders and decide whether this approach will be implemented on an ongoing basis. It would also be appropriate for Defence to consider, as part of this evaluation, whether an alternative approach would be preferable and explore whether the clarification of existing thresholds would be sufficient or whether legislative amendment is required.

### Recommendation 8

The Department of Defence should formally evaluate its two-step cryptography permit trial and decide whether the approach will be implemented on an ongoing basis. The evaluation should consider whether an alternative approach would be preferable and explore whether the clarification of existing thresholds would be sufficient or whether legislative amendment is required.

<sup>126</sup> Australian Universities Cryptography Researchers, submission 14, p. 2.

<sup>127</sup> University of Melbourne, submission 24, p. 2.

## SUPPLY TO A RELATED BODY CORPORATE

### Background

The current Defence guidance on supply indicates that '[s]upply must occur between one person (or in other words, a legal entity) and another person. For example, an employee of "Company A" located in Australia, emails DSGL technology to an employee of the same "Company A" who is located overseas, and the email is in the course of their duties as employees of the company, a permit would not be required because the supply is occurring within the same legal entity.'<sup>128</sup>

### Submission

In its submission, Northrop Grumman set out a scenario in which an individual on assignment in Australia is reassigned from their overseas home office (Entity A) to a specific legal entity (Entity B) within the corporate group for the duration of their international assignment. Both of the legal entities are part of the broader corporate structure and all are incorporated and located in a single country.<sup>129</sup> Northrop Grumman suggested that as the structure of many corporations can be complex, language indicating that the exception relating to supply within the same legal entity should be reviewed and, if possible, expanded to include supply between related body corporates.

### Discussion

The approach proposed by Northrop Grumman might be appropriate for entities operating in certain countries, but it is conceivable that such an approach could be used to circumvent the intent of the legislation where related body corporates operate in countries with interests that are not compatible with Australia's national interests. Although the Review is sympathetic to the apparent extra regulatory burden that is imposed upon multinational entities with related bodies corporate operating in different countries, it is not persuaded that there is a compelling case for legislative amendment at this stage.

## EXEMPTIONS FOR ANSTO OFFICERS

### Background

Subsection 10(3) of the DTC Act provides that an offence is not committed if DSGL technology is supplied by or to specified classes of persons, including members of the ADF; employees of the Australian Public Service, the Australian Federal Police, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service and the Australian Signals Directorate; and members of the police force of a state or territory of Australia; and where the supply occurs in the course of their duties. Section 15 provides similar immunities for brokering.

---

<sup>128</sup> Department of Defence, Defence Export Controls, *Supply of export-controlled goods and technologies*, <http://www.defence.gov.au/ExportControls/Supply.asp>.

<sup>129</sup> Northrop Grumman Australia, submission 43, p. 1.

## Submission

The Australian Nuclear Science and Technology Organisation (ANSTO) advised that officers of ANSTO were not currently included in these classes of person.<sup>130</sup> It advised that 'ANSTO has a legislated authority to act as a means of liaison between Australia and other countries in matters related to its activities, which commonly involve the development and application of DSGL-listed technologies. ANSTO submitted that there was sufficient justification for including ANSTO officers in the list of officials to whom the offences under the DTC Act do not apply when acting in the course of their duties.

## Discussion

Currently, ANSTO officers would be required to obtain permits under the DTC Act, which would seem excessive regulation for an agency of ANSTO's nature. The Review also notes that ANSTO staff are subject to the same general rules that apply to other Commonwealth officers regarding the disclosure of information. The Review is persuaded by ANSTO's submission.

### Recommendation 9

The Government should consider amending the *Defence Trade Controls Act 2012* to include employees of the Australian Nuclear Science and Technology Organisation in the offence exemptions of sections 10(3) and 15, where the activities occur in the course of their duties.

---

<sup>130</sup> ANSTO, submission 12, p. 2.

THIS PAGE IS INTENTIONALLY BLANK

# APPENDIX A: TERMS OF REFERENCE

## Background

Defence administers controls on the export of military and dual-use goods and technologies through four key pieces of legislation. The *Defence Trade Controls Act 2012* provides the legislative basis for the controls of the intangible supply, publication and brokering of defence and strategic goods and technology. The Act was enacted in 2012 to strengthen Australia's existing export controls and to align them with international best practice.

The Act underwent amendments in 2015 following extensive stakeholder consultation. One such amendment included the addition of a mechanism to provide for review of the operation of the Act after two years of the offence provisions being commenced, which occurred on 2 April 2016.

## Aim

The aim of the Review is to evaluate the operation of the DTC Act and deliver recommendations that ensure the Act is an effective component of Australia's export control regime that appropriately addresses current and future national security requirements.

The Review will also aim to ensure the Act provides appropriate levels of regulation and security for controlled technologies, aligns with international best practice for export controls, and is not unnecessarily restricting trade, research and international collaboration.

## Scope

The Review is mandated by section 74B of the Act:

The Minister must cause a review of the operation of this Act (other than Parts 3 and 4) to be undertaken as soon as possible after the second anniversary of the commencement of section 10 of this Act and afterwards at intervals of not longer than 5 years.

The persons undertaking the review must give the Minister a written report of the review.

The Minister must cause a copy of the report of the review to be tabled in each House of the Parliament within 15 sitting days of that House after the report is given to the Minister.

The Review is limited to the operation of the Act but subsection 74B(1) specifically excludes Parts 3 and 4 – that relate to the Defence Trade Cooperation Treaty between Australia and the United States of America – from scope of the review.

The Review will examine all other Parts of the Act to provide evidence-based, practical recommendations for improvements to the Act and supporting policy. In particular, the Review will consider:

- whether the Act is fit for purpose;
- whether there are any gaps in the Act's controls;
- whether any unintended consequences are resulting from the Act's controls; and
- any other matters considered relevant.

## **Consultation and delivery**

Stakeholder input on the operation and effectiveness of the Act is crucial to the review.

Accordingly, the review will involve extensive engagement with relevant stakeholders, including relevant Federal Ministers and government agencies, and representatives from industry, higher education and research sectors. This will occur through consultation, the release of papers, and receipt of submissions to ensure stakeholder views are considered before making recommendations.

The Review's final report will be provided to the Minister for Defence.

## APPENDIX B: LIST OF SUBMISSIONS

- 1 Columbus Group
- 2 Anonymous
- 3 Jeff Prcevich
- 4 Morgan Advanced Materials
- 5 Omnitech
- 6 Rafael Advanced Defense Systems Ltd
- 7 Richard Sawday
- 8 Australian Academy of Science
- 9 University of New South Wales
- 10 University of Tasmania
- 11 Air Power Australia
- 12 ANSTO
- 13 ATSE
- 14 Australian Universities Cryptography Researchers
- 15 Simulation Australasia
- 16 Stephen Hyde
- 17 Susan Hutchinson
- 18 Australasian Research Management Society
- 19 Deakin University
- 20 DMTC Ltd
- 21 Goal Professional Services
- 22 Murdoch University
- 23 Universities Australia
- 24 University of Melbourne
- 25 University of Technology Sydney
- 26 University of Western Australia
- 27 Australian National University
- 28 Group of Eight
- 29 RMIT
- 30 Association of Australian Medical Research Institutes
- 31 Export Council of Australia
- 32 Mark Lane
- 33 Queensland University of Technology
- 34 Saab Australia
- 35 University of the Sunshine Coast
- 36 Australian Research Council
- 37 University of Adelaide
- 38 CSIRO

- 39 Royal College of Pathologists Australasia
- 40 Thales Australia Limited
- 41 Boeing Australia Holdings
- 42 University of Wollongong
- 43 Northrop Grumman Australia
- 44 Confidential
- 45 Department of Foreign Affairs and Trade
- 46 Department of Defence
- 47 University of South Australia
- 48 National Tertiary Education Union
- 49 Australian Industry Group
- 50 Black Sky Aerospace
- 51 Flinders University
- 52 Michael Shoebridge
- 53 University of Queensland
- 54 Australian Rocketry
- 55 Equatorial Launch Australia

## **SUPPLEMENTARY SUBMISSIONS**

- 1 Australian Academy of Science
- 2 Australian Academy of Technology and Engineering
- 3 Australian National University
- 4 University of Adelaide
- 5 University of New South Wales
- 6 University of South Australia
- 7 University of Queensland
- 8 University of Sydney
- 9 Association of Australian Medical Research Institutes
- 10 Group of Eight
- 11 Queensland University of Technology
- 12 Science and Technology Australia
- 13 Universities Australia
- 14 University of Technology Sydney
- 15 Australasian Research Management Society
- 16 University of Wollongong
- 17 University of Melbourne
- 18 Northrop Grumman
- 19 Saab Australia
- 20 Goal Group

# APPENDIX C: LIST OF MEETINGS

## Sector meetings

2 May 2018, Australian Industry Group, Export Control Forum, Canberra  
9 May 2018, Australian Government Research Agencies Meeting, Canberra  
17 May 2018, Deputy Vice Chancellors – Research Meeting, Canberra  
17 May 2018, Defence Industry State and Territory Forum, Canberra

## Peak body representatives

7 May 2018, Head of Deputy Vice Chancellors – Research, by telephone  
29 August 2018, Group of Eight Chief Executive Officer, Canberra  
16 August 2018, Universities Australia Chief Executive Officer, Canberra

## Ministerial meetings

21 June 2018, Minister for Foreign Affairs, Canberra  
22 June 2018, Office of the Minister for Home Affairs, Canberra  
27 June 2018, Office of the Minister for Education and Training, Canberra  
15 August 2018, Office of the Minister for Trade, Tourism and Investment, Canberra  
12 September 2018, Minister for Defence, Canberra  
13 September 2018, Minister for Defence Industry, Canberra

## Departmental meetings

21 June 2018, Department of Industry, Innovation and Science, Chief Scientist, Canberra  
3 August 2018, Department of Defence, Assistant Secretary Defence Export Control, Canberra  
28 August 2018, Department of Defence, Secretary, Canberra  
30 August 2018, Department of Foreign Affairs and Trade, Canberra  
5 September 2018, Department of Home Affairs, Canberra

## Stakeholder meetings

9 August 2018, Dr Vanessa Teague, University of Melbourne, by telephone

## **PARTICIPANTS AT STAKEHOLDER ROUNDTABLES**

### **6 August 2018, Sydney**

- Australasian Research Management Society
- University of New South Wales
- University of Technology Sydney
- Royal College of Pathologists of Australasia Quality Assurance Programs
- University of Sydney
- University of Newcastle
- Western Sydney University
- Australian Industry and Defence Network (NSW)
- Goal Professional Services

### **7 August 2018, Brisbane**

- Queensland University of Technology
- University of the Sunshine Coast
- University of Southern Queensland
- The University of Queensland
- Southern Cross University
- Boeing Australia
- Black Sky Aerospace
- Australian Industry and Defence Network
- Australian Universities Cryptographic Researchers

### **13 August 2018, Melbourne**

- Universities Australia
- Deakin University
- Association of Australian Medical Research Institutes
- RMIT
- National Tertiary Education Union
- Monash University
- SME Defence Consulting
- Equatorial Launch Australia
- DMTC Ltd
- BAE Systems Australia
- Australian Industry and Defence Network (Victoria)

### **14 August 2018, Hobart**

- Department of State Growth
- Liferaft Systems Australia
- University of Tasmania
- Tasmanian Defence Advocate

### **22 August 2018, Perth**

- Murdoch University
- Curtin University
- University of Western Australia
- Edith Cowan University

**23 August 2018, Adelaide**

- Australian Universities Cryptographic Researchers
- Flinders University
- University of Adelaide
- University of South Australia
- ASC Pty Ltd
- Saab Australia Pty Ltd

**28 August 2018, Canberra**

- Australian Nuclear Science and Technology Organisation
- Australian National University
- Group of Eight
- Australian Research Council
- CSIRO
- Australian Academy of Science
- Science and Technology Australia
- University of Wollongong
- Griffith University
- University of Melbourne
- Australian Academy of Technology and Engineering
- Equatorial Launch Australia
- Northrop Grumman Australia
- Leidos Australia
- CAE
- Department of Foreign Affairs and Trade

THIS PAGE IS INTENTIONALLY BLANK



