4

Actions and recommendations

4.1   As has been discussed, the Australian Government already has a range of policies and initiatives in relation to the digital economy. In this chapter, drawing on themes highlighted in evidence received in this inquiry, the Committee points to actions that should be taken to ensure that Australia makes the most of the opportunities of the digital economy. These are:

- the need for a cohesive, whole-of-government approach;
- the need to build digital awareness into Australia's education system, including for those already working;
- the need to rebuild systems, designing processes from the ground up;
- the need to build cyber resilience; and
- the need to work closely with trading partners and multinational organisations.

The need for a cohesive approach

4.2   As was highlighted in chapter 2, the broad range of agencies that run sometimes overlapping trade and the digital economy initiatives can create confusion. A cohesive, all-of-government, streamlined approach, including a single information portal, would alleviate much of that confusion and help Australian businesses find opportunities for growth.

4.3   Several witnesses highlighted that the there is a barrier for many Australian businesses, particularly SMEs, in that they are unable to easily access the information that might help them better utilise the digital economy.

4.4   The scale of the problem was highlighted in the Home Affairs submission:

> Over 40 000 Australian businesses engage in international trade, with the general public also increasingly using e-commerce to buy overseas goods. These transactions are regulated by more than 30 government agencies that administer approximately 200 pieces of legislation.[1]

4.5   While SMEs can potentially benefit from the opportunities of the digital economy, knowing what those are and how they can be used remains a problem:

> … there are issues around knowing what government and private sector resources are available. AusIndustry and Austrade, for example, provide a number of useful resources and advice to small businesses and start-ups looking to go abroad, but a number of the businesses that would benefit from them don't often know that they are available.[2]

4.6   This was highlighted by Mr Colvin from the Global Innovation Forum, discussing conversations he'd had with Australian businesses:

> One of the things that came out repeatedly […] is that there's not a single window or a one-stop shop for start-ups or small businesses to go to in the government and understand the scope of resources and funding programs [...]. I know business.gov.au is trying, but that sort of […] single window doesn't exist.[3]

4.7   Ms Lamb from the National Retail Association also made this point, arguing that government information on digital economy options for retailers 'is not all in one spot. It's not as easy to locate'.[4]

4.8   ANZ noted that, while there is plenty of information provided by the Government, it is not centralised. To address that, ANZ's Mr Evans suggested:

> I think there's a lot the government could do in providing a portal to make it easier to access the information. More and more people, particularly the small companies, don't have large R&A developments. This is mums and dads, or a couple of guys in a garage with a good idea. They don't have the resources to spend time researching it or to have people do it for them. So we've just

---

1   Home Affairs, *Submission 15*, p. 4.

2   Mr Colvin, Global Innovation Forum, National Foreign Trade Council Foundation, *Committee Hansard*, 19 October 2017, p. 1.

3   Mr Colvin, Global Innovation Forum, National Foreign Trade Council Foundation, *Committee Hansard*, 19 October 2017, p. 4.

4   Ms Lamb, National Retail Association Ltd, *Committee Hansard*, 17 August 2018, p. 27.

> got to find a way to help it be easier for them to understand where they may be competitive, where they should focus their efforts and how they can complete those transactions in a compliant way.[5]

4.9   Similarly the AI Group praised some of the work done by Austrade, but noted that the 'general advice on their website appears to ignore the existence of digital technologies'.[6]

4.10   The problem with the lack of a single point of contact was highlighted by this illustration:

> We hear from start-ups and small businesses that they don't know where to turn either to comply with regulations or when things go wrong. We met a CEO of a small business in London who had her shipment stuck in customs in the United States because there was a problem with the tariff classification code. It took her — the founder at CEO level — three days to work this out simply because she didn't know who to talk to. She kept googling and finally found some poor woman at US customs who was able to help her out.[7]

4.11   The role of Ambassador for Cyber Affairs, located within DFAT, was designed to have a single identifiable person with broad responsibility for Australia's international cyber engagement. Dr Feakin, the first appointee to the position, described the role as:

> … to have a senior representative from government who coordinates across the whole of the Australian system — the private sector and civil society — to ensure that we have the appropriate level of representation in the international system. It was born out of the reasoning that the digital space is not only important for trade but also becoming an increasingly important part of all of our foreign interactions.[8]

4.12   As such, amongst other responsibilities, the Ambassador chairs quarterly meetings of all the agencies who have any involvement in cyber issues, with the aim of ensuring a coordinated approach.[9]

4.13   The *International Cyber Engagement Strategy*, published in October 2017, 'sets a pretty ambitious agenda for Australia across the whole spectrum of

---

5   Mr Evans, ANZ, *Committee Hansard*, 17 August 2018, p. 34.

6   AI Group, *Submission 9*, p. 7.

7   Mr Colvin, Global Innovation Forum, National Foreign Trade Council Foundation, *Committee Hansard*, 19 October 2017, p. 4.

8   Dr Feakin, Ambassador for Cyber Affairs, *Committee Hansard*, 9 February 2018, p. 1.

9   Dr Feakin, Ambassador for Cyber Affairs, *Committee Hansard*, 9 February 2018, p. 4.

what we term "cyber affairs", including, notably, Digital Trade as the first chapter.[10]

4.14 Within the broader domestic framework, the forthcoming Digital Economy Strategy is designed to have a similar role; to reduce the fragmentation of Australia's digital economy approach, and bring together information and initiatives.[11]

4.15 The rationale for the Digital Economy Strategy is explicitly to bring together the range of programs already in existence:

> The Government already supports action on a diverse range of digital economy initiatives across multiple agencies. A key purpose of the strategy will be to draw together, complement and build on these existing initiatives. […] To make sure we stay up to date, the strategy will evolve over time.
>
> Trade issues, particularly digitally-enabled trade, will be an important component of the strategy. While a significant proportion of e-commerce is still conducted domestically, the nature of digital trade means that Australian businesses of all sizes can readily target markets around the world. This potential extends even to small businesses which would not previously have had the capacity to develop overseas markets. Australian business can leverage worldwide reputational advantages for Australia as a producer of safe, high quality products across a range of sectors.[12]

The need to build digital awareness

4.16 In the same way that cyber security and cyber resilience need to be integral to both government and business operations, education and information about digital technologies needs to be given a greater priority. From education at schools through to reskilling workers and business owners, understanding of the digital economy should be regarded as a vital aspect of 21st century life.

4.17 As Mr Alexander of the Digital Transformation Agency emphasised, it is vital for Australia's future economic interests that this focus begins early:

---

10   Dr Feakin, Ambassador for Cyber Affairs, *Committee Hansard*, 9 February 2018, p. 1.

11   Dr Chris Locke, First Assistant Secretary, Portfolio Policy and Innovation Strategy Division, Department of Industry, Innovation and Science, *Committee Hansard*, 9 February 2018, p. 24.

12   DIIS, *Submission 3*, p. 8.

> We are not getting kids into science and technology. We are
> particularly not getting women into science and technology. We
> have to do more of that to get them early. By university it is too
> late. If they have not studied it at school and if they have not gone
> through, it is a real challenge to get kids into science and
> technology past school.[13]

4.18   To respond to these challenges, AustCyber, as part of its role as the cyber
        security growth centre, spends around half its time working on education
        programs and initiatives. While not every student will have a career in
        cyber security:

> … it's making sure that all students have at least some skill sets in
> cyber security because cyber will be a component of every job in
> the future. In fact, we have lots of evidence to prove that in fact
> most jobs in the economy right now do require some baseline level
> of cyber security education.[14]

4.19   Beyond school, Australian TAFEs now offer a nationally consistent
        certificate IV in cyber security, and courses at the university level are also
        being developed and offered. Importantly, there is an expansion of focus
        from technical skills to the broader skills that are required to manage
        cyber security risks, including on topics such as legal issues, risk
        management, financial management and general management skills. [15]

4.20   Facebook recommended a series of 'pro-innovation policies', including
        STEM degree enrolment and completion incentives to encourage an
        adequate workforce, including women and other underrepresented
        groups in the sector.[16]

4.21   Business emphasised that new opportunities in the digital realm require
        new skillsets, and consequently a focus on those in the education and
        training sectors.[17]

4.22   The consultation process for the government's Digital Economy Strategy
        found that the issue most raised by stakeholders was the need for
        improved digital skills:

> No matter what your sector, digital skills is seen as the biggest
> issue. […] actually having the capacity in businesses to have the
> right types of skills to support digitally enabled businesses and
> accessing digital markets is the critical thing. So businesses need to

---

13   Mr Alexander, Digital Transformation Agency, *Committee Hansard*, 9 February 2018, p. 15.
14   Ms Price, AustCyber, *Committee Hansard*, 28 June 2018, p. 1.
15   Ms Price, AustCyber, *Committee Hansard*, 28 June 2018, p. 1.
16   Facebook, *Submission 6*, p. 5.
17   Ms Lamb, National Retail Association Ltd, *Committee Hansard*, 17 August 2018, p. 23.

know that they need those skills and suppliers of skills need to know what sorts of skills should actually be supplied. There needs to be a market that settles that in an effective way. That is a big story, from education to business incentives, but that is the No. 1 topic that comes out.[18]

4.23   Given that, there is a role for the government to help Australian businesses bring their practices into the digital economy:

> There's an opportunity for the Australian government to emphasise to small businesses… about the technologies and the resources that are available to help put those businesses on a footing to go global.[19]

4.24   The Export Council made this point, arguing that many Australian businesses are simply unaware of their options, and that the government should focus on providing that information:

> Education is key to enabling businesses to start on the right path. But all too often, businesses rely on trial and error to work out what they need for international success. The government should fund education and training programs for start-ups in the digital economy to help them go global.
>
> The government must strengthen its support for Australian digital businesses to succeed internationally. Too often Australian businesses are not alert to the opportunities offshore or not willing to take the risk to realise those opportunities. Adequately funding the Export Market Development Grant (EMDG) scheme, and increasing resources for Austrade, are essential… to give businesses confidence and certainty in pursing international marketing activity. For a business, not knowing how much of its expenditure will be rebated creates risk and undermines those objectives.[20]

4.25   Relatively new areas such as artificial intelligence and machine learning, Innovation and Science Australia has identified, are 'significant area[s] of competitive advantage where Australia is being left behind, and more work needs to be done building on Australia's strength in that'.[21]

4.26   To address the lack of engagement amongst Australian businesses, the Export Council recommended a 'concerted awareness campaign that's

---

18   Dr Locke, DIIS, *Committee Hansard*, 9 February 2018, p. 24.

19   Mr Colvin, Global Innovation Forum, National Foreign Trade Council Foundation, *Committee Hansard*, 19 October 2017, p. 4.

20   Export Council of Australia, *Submission 10*, p. 4.

21   Dr Locke, DIIS, *Committee Hansard*, 9 February 2018, p. 24.

followed up by education into the benefits of, and then how to do, business internationally'.[22]

The need to rebuild systems

4.27   As discussed in chapter three, witnesses highlighted that a mere application of digital technology to analogue systems will bring small benefits, but to make the most of the digital economy, governments—like private industry—need to rebuild their approach from the ground up. This change means not just improving current systems by digitising them, but redesigning systems on the basis of digital technologies. This is an essential aspect of addressing the challenges and opportunities presented by the digital economy. Processes and systems must be reengineered and re-imagined for maximum advantage.

4.28   ACCI noted their recommendation that DFAT seek a 'digital by default' approach to trade agreements, particularly for documentary requirements such as evidence of origin information.[23]

4.29   DIIS highlighted that Australia's approach to digital components of trade agreements has grown more sophisticated as the digital economy has:

> The nature of [e-commerce] provisions has evolved over time, with earlier FTAs focussing on paperless trading, protection of online consumers, and excluding electronic transmissions from customs duties. Importantly, more recent FTAs have also included provisions concerning the protection of personal information, cross border data flows, disclosure of source code and location of computing facilities.[24]

4.30   DIIS noted that it works closely with DFAT on FTA negotiations, including advising on e-commerce and other relevant issues.[25]

4.31   So too does Home Affairs, particularly in the light of the single-window proposition that department is currently building.[26]

4.32   In recognition of the centrality of the digital economy to trade overall, agencies like Austrade are incorporating their work on digital goods and

---

22   Mr Baker, Export Council of Australia, *Committee Hansard*, 15 February 2018, p. 5.

23   ACCI, *Submission 18*, p. 2.

24   DIIS, *Submission 3*, p. 10.

25   DIIS, *Submission 3*, p. 10.

26   Ms Sawczuk, Home Affairs, *Committee Hansard*, 10 May 2018, p. 13.

services directly into the specific sector-based teams, rather than considering digital issues as a separate area.[27]

4.33   Some of the work currently being done in relation to the trade system is in fact moving towards a reimagined digital approach, including the single-window system proposed by Home Affairs:

> They are doing exactly this, which is to say, 'What are we doing? What is the problem we are solving?' How do we go back to first principles and say, 'What is the problem we are solving?' If we were greenfields, how would we do it? Then we have the challenge, which is that we have to overlay that with the complications of legislation and all of the various things we have and say, 'Well, in a pragmatic and practical world bound by some of these things, which are really hard to change, what would we do?'[28]

4.34   Crucially, the system Home Affairs is proposing is being built on the basis of consultation with industry: 'Industry support, co-design and co-investment will be critical and will assist in building our international trading future'.[29]

4.35   Evidence was received which emphasised the importance of interoperability, noting that jurisdictions will implement single windows to address local requirements. In this regard harmonisation does not produce a desirable outcome, whereas interoperability ensures that compatible technologically neutral systems can exchange feature-rich data across borders.[30]

The need to build cyber resilience

4.36   There is significant room for improvement in Australia's response to the risks posed by cyber threats. Robust cyber security measures promote trust and user confidence, providing an environment where digital trade can flourish and drive economic growth.[31]

4.37   The importance of a management focus on, not just a technical response to, cyber security and resilience was emphasised by AustCyber's Ms Price:

27   Mr Rees, Austrade, *Committee Hansard*, 9 February 2018, p. 20.

28   Mr Alexander, Digital Transformation Agency, *Committee Hansard*, 9 February 2018, p. 16.

29   Mr John Gibbon, Acting First Assistant Secretary, Trade and Customs Division, Department of Home Affairs, *Committee Hansard*, 10 May 2018, p. 8.

30   Mr Evans, ANZ, *Committee Hansard*, 17 August 2018, p. 30.

31   *Australia's International Cyber Engagement Strategy*, p. 23.

> So that governance component is critical to make sure that
> decision-makers are aware of their accountabilities and
> responsibilities in seeing that cyber-risk is not something that is a
> tick-and-flick but is in fact quite complex. It's complex, of course,
> because of the way in which we've digitised our world. It's not
> enough to simply receive a report and see the dashboard with the
> reds going down and the greens going up. There is so much more
> to this, which means that that care factor and the culture around
> encouraging learning are very important.[32]

4.38   Similarly, building cyber security and resilience into your overall
        approach is ideal, if not always seen in practice:

> Security by design is always the preference. It's much harder to
> retrofit security when it comes to IT architecture. It is similar to
> when you build a building: it is smarter to think about those
> things at the time. I would say to you that that is a process of
> maturation in government, just as it is in business. The tech
> industry generally has taken a much longer time than anyone
> would have hoped to build security into the foundational products
> they have.[33]

4.39   AI Group supports AustCyber's initiatives, but warns regulatory and
        policy frameworks should carefully balance opportunity and risk, and be
        consistent with the Cyber Security Strategy to ensure businesses continue
        to develop and invest in cyber security technology in Australia.[34]

4.40   It is important to focus more on cyber resilience than on a narrow
        approach to cyber security:

> … we're moving our discussion from talking about security to
> resilience, and that's important, because you can't always be
> secure but you can make yourself more resilient. We're moving
> away from a compliance culture to a risk culture and we're
> moving away from talking about cyber security as a threat to
> talking about it as an opportunity.[35]

4.41   The key, as in other challenges and opportunities presented by the digital
        economy, is in providing education and information, and helping both
        businesses and governments recognise the centrality of cyber security and
        resilience:

---

32   Ms Price, AustCyber, *Committee Hansard*, 28 June 2018, p. 2.

33   Mr MacGibbon, ACSC, *Committee Hansard*, 10 May 2018, p. 3.

34   AI Group, *Submission 9*, p. 9.

35   Mr MacGibbon, ACSC, *Committee Hansard*, 10 May 2018, p. 1.

It's important […] that we make sure that that is the case right now, so that people do have the chance to be educated and learn about why cybersecurity is an important factor of life now. But, over time—over the next couple of years not over the next decade—we do need to normalise it. We need to make sure that we get to a much quicker position of it being an essential part of doing business—like where we were 15 years ago with the workplace health and safety situation […] It's making sure that, from a governance point of view, the accountabilities are understood and it's understanding that this is much more a risk-management endeavour than it is a compliance endeavour.[36]

The need to work with global partners

4.42   A theme stressed by many of the inquiry's witnesses was the importance of Australia working with its trading partners and multilateral organisations to build a consistent and appropriate trade system that works in the digital economy.

4.43   On a broad level, witnesses argued that Australia should continue to emphasise the importance of open trade rather than protectionism:

To maintain global momentum for trade, the government must continuously pursue trade agreements that increase openness—at the multilateral, plurilateral and bilateral levels. Where necessary, it must be prepared to defend global trade rules by launching international legal action when these rules are violated, even by key allies.[37]

4.44   DFAT outlined some of the roles that Australia is taking in advocating for 'liberalising outcomes for electronic commerce' within the WTO:

While existing WTO Agreements such as the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS) cover all trade in goods and services, countries like Australia want to see the WTO negotiate multilateral rules specifically focused on electronic commerce, which could complement existing obligations in the GATT and GATS. New rules could ensure, for example, that all WTO Members recognise electronic signatures and do not prescribe the means by which two parties to an electronic transaction authenticate that transaction.

---

36   Ms Price, AustCyber, *Committee Hansard*, 28 June 2018, p. 2.

37   Export Council of Australia, *Submission 10*, p. 5.

Australia would also like to see rules governing how WTO Members deal with unsolicited electronic messages (spam), and in more complex areas such as the free flow of data and limiting requirements to store data in particular markets.[38]

4.45   The WTO is the best forum for these matters to be decided:

…new trade rules on the digital economy, be they on electronic commerce, technical barriers to trade, intellectual property, international regulatory cooperation or international standards […] should best be agreed and adopted at the World Trade Organisation. […] This is for reasons of legitimacy as well as inclusion and so that the economic impact of these rules is felt as widely as possible and can benefit the greatest number of people. Another reason that the WTO is the right place for these rules rather than, say, in FTAs is because of the importance of the public policy exceptions. History has shown us that FTAs have a very weak record on dispute settlement, whereas the dispute settlement system of the WTO is the jewel in the crown.[39]

4.46   Australia played a lead role in digital commerce discussions at the WTO Ministerial Conference in Buenos Aires in December 2017:

[W]e led the recent initiative on e-commerce at the WTO. That initiative attracted the support of 71 members—about two-thirds of global trade...

4.47   Australia also prioritises e-commerce in trade negotiations, including the TPP11, the Regional Comprehensive Economic Partnership, the Pacific Alliance bilateral treaty, and free trade agreements with Indonesia and Hong Kong.[40]

4.48   On a practical level, Standards Australia led a harmonisation project within APEC for the movement of data across borders, identifying the standards that are required to enable trade amongst the 16 countries.[41]

---

38   DFAT, *Submission 11*, p. 4.

39   Mr Simon Lacey, Vice President, Global Government Affairs, Trade Facilitation and Market Access, Huawei Technologies, *Committee Hansard*, 9 February 2018, p. 35.

40   Mr George Mina, First Assistant Secretary, Department of Foreign Affairs and Trade, *Committee Hansard*, 9 February 2018, p. 20.

41   Mr Varant Meguerditchian, General Manager, Stakeholder Engagement, Standards Australia, *Committee Hansard*, 9 February 2018, p. 28.

Trade agreements in the digital economy

4.49   DFAT also explained that Australia's trade agreements are seen as 'living agreements' which can be reviewed and updated as changes in the trade environment require:

> We have just undertaken a very comprehensive amendment of our free trade agreement with Singapore… The agreement was originally struck in 2000. Last year we amended it. One of the big things that we upgraded in that agreement was the treatment of e-commerce. We did include in there a whole range of these rules relating to data that had not been in the original agreement simply because it wasn't an issue back in 2000.[42]

4.50   Standards Australia is working to promote the harmonisation of digital standards in the Indo-Pacific region.[43]

4.51   A further way in which Australian trade agreements can help businesses—particularly SMEs—is through working with trading partners to further the WTO's Trade Facilitation Agreement, which requires countries to develop a guide for overseas-based businesses to do business in their countries.[44]

Digital capacity in trading partners

4.52   Australian businesses will also have greater opportunities if all countries have the infrastructure the digital economy requires. As discussed in chapter 2, the Australian Government, through DFAT, has initiatives in place to assist some of Australia's trading partners to improve their digital infrastructure. More, however, can be done:

> The implications of government, for instance, prioritising assistance to countries in the Asia-Pacific region in terms of their digital capability and addressing cyber security issues are right on track in terms of assisting our METS sector to be able to gain the benefits of their domestic investments in overseas markets. It was quite frustrating to them to be operating in far-flung places in the world and having to revert back to fairly basic, paper based systems to enable them to exist in those areas.[45]

42   Mr Baxter, DFAT, *Committee Hansard*, 7 September 2017, p. 7.

43   Dr Feakin, Ambassador for Cyber Affairs, *Committee Hansard*, 9 February 2018, p. 1.

44   Mr Colvin, Global Innovation Forum, National Foreign Trade Council Foundation, *Committee Hansard*, 19 October 2017, p. 5.

45   Dr Heyward, METS Ignited, *Committee Hansard*, 8 February 2018, p. 3.

Data duties

4.53   For the maximum benefits of the digital economy, electronic transmissions must continue to be exempt from duties as they cross international borders. Currently, a WTO moratorium on countries imposing duties on electronic transmissions is renewed every two years. Stakeholders, including the Australian Government, want to see this policy made permanent.

4.54   As the Export Council argued, the two year process is 'inadequate', and the agreement should be made permanent 'sooner rather than later'.[46]

4.55   Huawei made the case for the free flow of data across borders, arguing that:

> … we all win in a world where the internet is global, open and free since a global, open and free internet allows for the free flow of ideas and the spread of new technologies and innovation. It also goes a long way to ensuring the future unencumbered growth of the digital economy and all of the benefits this can bring mankind.[47]

4.56   The Information Technology and Innovation Foundation (ITIF) described the free flow of data as 'the central feature of the global digital economy' and policies protecting it as critical.[48]

4.57   This reflects the feedback DFAT has received from businesses, who note the value of data:

> … we keep hearing from business that, in the trade law and trade policy spaces […] the data is the product and the freedom of movement of that data needs to be the objective.[49]

4.58   DFAT noted that making this moratorium permanent is Australian government policy.[50] At the WTO Ministerial Conference in Buenos Aires in December 2017, Australia—along with Singapore and Japan—led a movement to make the moratorium permanent, which garnered the support of 71 countries.[51]

---

46   Export Council of Australia, *Submission 10*, p. 3.

47   Mr Lacey, Huawei Technologies, *Committee Hansard*, 9 February 2018, p. 34.

48   ITIF, *Submission 21*, p. 4.

49   Mr George Mina, First Assistant Secretary, Department of Foreign Affairs and Trade, *Committee Hansard*, 9 February 2018, p. 26.

50   DFAT, *Submission 11*, p. 4.

51   Mr Mina, DFAT, *Committee Hansard*, 9 February 2018, p. 26.

Data localisation and flow

4.59   Data localisation laws are requirements that certain types of data are stored in country. Australia, like many countries, has some data storage requirements. On the whole, witnesses suggested that such requirements should be kept to a minimum, and that Australia should work to make this the norm.

4.60   The Export Council argued that data localisation laws were misguided:

> Governments must … agree a framework that strikes the right balance between protecting data and allowing it to flow freely between borders. Currently many governments use privacy as an excuse to require data to be held within their jurisdiction. This is fig leaf for protectionism.[52]

4.61   ITIF described data localisation requirements as 'a new barrier to global digital trade', noting that:

> Cutting off data flows or making such flows harder or more expensive puts foreign firms at a disadvantage. This is especially the case for small and solely Internet-based firms and platforms that do not have the resources to deal with burdensome restrictions in every country in which they may have customers.[53]

4.62   The Export Council highlighted that it's not only big companies like Google or Facebook who rely on cross-border data flows, but very small businesses too.[54]

4.63   Indeed, illustrating the breadth of the digital economy, a report by McKinsey Global Institute estimated that 75% of the value of data flows goes to traditional industries such as manufacturing.[55]

4.64   DFAT noted the disadvantages of data localisation requirements and its own work with trading partner nations to discourage the adoption of these policies:

> … some governments in our region are putting in place measures that have the potential to significantly dampen international digital trade such as restrictive cyber security measures, onerous privacy requirements, data localisation requirements and censorship. The Department engages these governments to

---

52   Export Council of Australia, *Submission 10*, pp 3 – 4.

53   ITIF, *Submission 21*, p. 5.

54   Mr Baker, Export Council of Australia, *Committee Hansard*, 15 February 2018, p. 1.

55   Mr Nigel Cory, Senior Trade Policy Analyst, Information Technology and Innovation Foundation, *Committee Hansard*, 21 June, p. 1.

highlight the importance of not unduly undermining trade
opportunities.[56]

4.65   Australia's position on data storage when negotiating trade agreements is:

> … that data should be allowed to flow freely across the border and
> there should be no rules that mandate the storage of data in a
> particular territory. The starting point [is] complete flexibility for
> business as to how its data is managed [and] flexibility for
> governments to have rules and regulations for important policy
> purposes such as privacy protection.
>
> Some of the security agencies… may need to impose rules on how
> data in Australia is managed. That's something that we insist on in
> our trade agreements. Another [consideration] relates to
> prudential reasons. The prudential agencies in Australia may say,
> 'If you're involved in financial transactions, if you're providing
> financial services in Australia, you've got to meet the following
> rules for prudential reasons'. We make sure that that sort of
> flexibility is allowed as well. There is a balance there that we really
> take into negotiations.[57]

Data measurement

4.66   Adequately measuring the scope of digital economy activity is crucial to
policymaking. The ITIF pointed to some examples Australia could draw
on, in conjunction with its trading partners and multilateral organisations,
to improve the quality of this data. These included:

- surveys of sellers regarding their overseas sales is 'one of the current
  best methods for measuring the value of cross-border e-commerce and
  digital trade';

- the OECD model survey on ICT access and use includes questions
  about online purchases, to which could be added questions cross-
  border purchases or sales;

- similarly, Eurostat's 'ICT in Enterprises' survey could, with the
  addition of more targeted questions, prove useful; and

- a United States Department of Commerce study into measuring the
  value of cross-border data flows provides recommendations for
  Australia to consider.[58]

4.67   The ITIF therefore recommended that Australia:

---

56   DFAT, Submission 11, p. 3.

57   Mr Baxter, DFAT, *Committee Hansard*, 7 September 2017, p. 6.

58   ITIF, *Submission 21*, pp 12 – 13.

> … push multilateral organisations, such as the WTO and the
> OECD, to track barriers to cross-border data flows and digital
> trade in order to document the extent of their use and to contribute
> to further analysis of how they impact digital trade.[59]

4.68   DIIS noted the importance of internationally consistent standards, including via the World Trade Organisation Treaty on Technical Barriers to Trade, which requires harmonisation and the adoption of international standards where possible. DIIS has responsibility for Australia's implementation of the treaty.[60]

Conclusion

4.69   Throughout this inquiry, the Committee heard from many Australians and organisations who have already benefited from the digital economy. Overall, evidence suggests that Australia is well-placed for the ongoing changes and challenges that the digital economy will bring.

4.70   However, the Committee also heard concerns that Australia's policy response to these changes is too fragmented, with many different agencies having separate areas of responsibility. While Australia's cyber security policy has been centralised in the Australian Cyber Security Centre, similar levels of coordination in relation to digital trade do not yet exist. The good work that is being done by different agencies is undercut by the difficulty businesses, especially SMEs, have in finding information on export requirements or assistance in the form of grants they can use to build their business.

4.71   The single-window trade approach being developed will assist in this regard and will reduce the regulatory burden on Australian businesses. Therefore, the Committee encourages the Government to continue with this program as quickly as possible. One of the key themes the Committee heard throughout this inquiry was the expansion of opportunities which the digital economy can offer for small businesses, who can now sell their goods and services to the world.

4.72   The Committee was pleased to hear about programs proposed to encourage young Australians to develop the cyber skills necessary for the 21st century, but equally emphasises that digital skills are workplace skills. All Australians should have the opportunity to access the education and training required for their ongoing participation in the workforce.

---

59   Mr Cory, ITIF, *Committee Hansard*, 21 June, p. 2.

60   DIIS, *Submission 3*, p. 7.

4.73   While some witnesses expressed mixed feelings about the readiness of Australia's international and trade negotiators to operate in the digital economy, the Committee notes that Australia has played a lead role in recent multilateral discussions on data flow, creating international standards and building international agreements that can adapt to the digital economy.

4.74   Given the fundamental importance of cyber security and resilience to the operation of the digital economy, the Committee commends the creation of the Australian Cyber Security Centre and the Australian Government's ongoing commitment to improving cyber security measures. The Committee believes that the Australian Government has an important role to play in leading the way on cyber issues, and encourages an increased incorporation of cyber security and resilience measures into broader government activities.

Recommendation 1

4.75   **The Committee recommends that the Australian Government, as a matter of priority, creates a single <u>portal of information</u>, with particular regard to exporting digital goods and services, including information about the development of digitally native processes.**

Recommendation 2

4.76   **The Committee recommends that the Australian Government, as a matter of priority, creates a single <u>window trading system</u>, with particular regard to exporting digital goods and services. This single window must be developed with a focus on interoperability to ensure rich data flows can be maintained and transmitted across borders.**

Recommendation 3

4.77   **The Committee recommends that the Australian Government release its Digital Economy Strategy.**

Recommendation 4

4.78   **The Committee recommends that the Australian Government continue to take future workforce needs into account in Australia's education system, from school through to tertiary education.**

Recommendation 5

4.79   **The Committee recommends that the Australian Government investigate options to fund and deliver training for those already in the workforce, to give them the skills to fully participate in the digital economy.**

Recommendation 6

4.80   **The Committee recommends that the Australian Government continue to promote digital trade standards, both technical and regulatory, with an emphasis on openness, technological neutrality and interoperability.**

Recommendation 7

4.81   **The Committee recommends that the Australian Government continue to support a permanent moratorium on duties for data flow.**

Recommendation 8

4.82   **The Committee recommends that the Australian Government work within the WTO to develop an internationally consistent system of measuring data flow.**

Recommendation 9

4.83   **The Committee recommends that the Australian Government ensure that all Commonwealth agencies comply with the Australian Signals**

Directorate's Essential Eight cyber security and resilience mitigation strategies.

Recommendation 10

4.84 **The Committee recommends that the Australian Government investigate ways to assist Australian SMEs to improve their cyber security awareness and resilience levels.**

Recommendation 11

4.85 **The Committee recommends that the Australian Government require all agencies when developing policy, legislation or trade agreements to consider whether what is proposed is technologically neutral and whether it could create barriers to the digital economy, including by limiting interoperability.**

Mr Ken O'Dowd MP

Chair

September 2018