HOME AFFAIRS PORTFOLIO
DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Senate Select Committee on Financial Technology and Regulatory Technology

5 March 2021

QoN Number: 01

Subject: Risk assessments for acquisitions

Asked by: Susan McDonald

Question:

In the Department of Home Affairs/AUSTRAC submission you noted that the Dept of Home Affairs, along with other agencies, provides advice to Treasury regarding foreign investment applications. You stated that when providing advice:
"The Department undertakes risk assessments on a case-by-case basis where an acquisition may involve foreign investment in a critical infrastructure sector, such as banking and finance. These assessments consider the risk of espionage, sabotage and coercion, including in relation to the asset's systems and data."
a. This is undoubtedly important work. Can you expand further on this process in terms of our capacity to do these assessments en masse?
b. Does this process effectively and efficiently work to both ensure security and facilitate investment?
c. Would all potential foreign investments in fintech and regtech be subjected to this level of risk assessment?
d. What about fintechs based outside of Australia that operate here? Are risk assessments being done on those fintech businesses, particularly ones with substantial levels of customer data? If not are we in a situation where entities that merely invest in fintechs are being more stringently assessed for risk than entities actually operating in Australia but based outside of the country?
e. How does this risk assessment process align with the Global Business and Talent Attraction Taskforce's focus on "attracting high-yield businesses and exceptionally talented individuals to Australia along with their ideas, networks and capital". Are there competing goals/interests in this respect?

Answer:

a. The Department of Home Affairs provided advice on 614 foreign investment cases during the 2019/20 financial year.
   Home Affairs has processes in place to ensure that a proportionate approach is taken to individual cases, with greater time and resources devoted to those cases that are likely to present significant risks.

b. The Department of Home Affairs' advice to the Treasury is solely focused on the extent of national security risk associated with a foreign investment transaction. It is the Treasurer's role, with the advice of the Foreign Investment Review Board and the Treasury, to balance the range of national interest considerations associated with each case.

c. Yes, where the investment meets the thresholds for either a national interest or national security review under the *Foreign Acquisitions and Takeovers Act 1975* (FATA). These thresholds differ depending on the nature of the transaction and the investor.

d. Yes, where the investment triggers either a national interest or national security review under the Foreign Acquisitions and Takeovers Act 1975 (FATA) or a relevant approval process under the *Financial Sector (Shareholdings) Act 1998*.

   Businesses based overseas, but operating in Australia, are generally treated the same as an investment in a wholly Australian business. New businesses entering the Australian market are also captured by the foreign investment framework, with similar thresholds applying.

e. The foreign investment review framework is intended to ensure the flow of foreign investment into Australia continues, while simultaneously ensuring a range of national interest considerations (including national security) are taken into account.

HOME AFFAIRS PORTFOLIO
DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Senate Select Committee on Financial Technology and Regulatory Technology

5 March 2021

QoN Number: 02

Subject: Digital economy

Asked by: Susan McDonald

Question:

In the Department of Home Affairs' submission you noted that while we continue to build our digital economy, "cyber threats continue to grow in sophistication, scale and impact".
a. How do we manage these threats as our digital economy becomes an increasingly large and important part of our overall economy?
b. Do we just have to accept that our digital economy is always going to be more vulnerable than other parts of the economy?

Answer:

Australia's Cyber Security Strategy 2020 outlines how the Australian Government is managing the increasing cyber security threat to the digital economy. Government, businesses and the community all have essential roles to play.

The $1.67 billion Strategy underpins Australia's approach to deterring, preventing, disrupting and responding to cyber security threats.

- *Disrupt* – The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, introduced to Parliament on 3 December 2020, will enhance law enforcement powers to combat serious online crime including on the dark web. Australia is also taking a leading role in negotiations on the Budapest Convention to streamline international crime cooperation between parties and enhance cross-border access to data by Australian law enforcement agencies.

- *Protect* – On 10 December 2020, the Government introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to Parliament to uplift cyber security protections for essential services. The Government is now considering what additional legislative reforms are necessary to protect

businesses in the broader digital economy, consistent with the Government's goal of being a leading digital economy by 2030.

- *Detect* – the Government has invested $1.35 billion in the Cyber Enhanced Situational Awareness and Response (CESAR) Package to identify more cyber threats, disrupt more foreign criminals, and bolster the Australian Signal's Directorate operational capabilities.

- *Respond* – the Government has invested $89.9 million to bolster the Australian Federal Police's ability to investigate and prosecute cyber criminals. The Government is also making additional support available to victims when cyber security incidents do occur. This includes $6.1 million to bolster services to victims of identity and cybercrime, and $12.3 million to extend the Australian Cyber Security Centre's 24/7 cyber security helpdesk.

Digital economies experience different types of vulnerabilities than other parts of the economy and addressing these vulnerabilities requires different responses. The deterrence, prevention, detection and responsive measures outlined in the Strategy will enable the Government, in partnership with businesses and the community, to build a prosperous and secure digital economy.

HOME AFFAIRS PORTFOLIO
DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Senate Select Committee on Financial Technology and Regulatory Technology

5 March 2021

QoN Number: 03

Subject: Digital Business Plan

Asked by: Susan McDonald

Question:

I was also really interested to read this excerpt from the DHA/AUSTRAC submission: "The inclusion of trust and security as a key pillar of the $800M Digital Business Plan is an acknowledgement that economic and security outcomes are inextricably linked, and that trust and security are now essential enablers of economic activity".
a. In many ways this is really the crux of what I wish to explore further. Is there anything more you can add regarding the link between trust and security, and their role as essential enablers of economic activity?
b. Can you explain their role as a "key pillar" in the plan?

Answer:

Cyber security threats are widely acknowledged to be a serious business risk and can have a significant impact on economic growth. In 2019 the World Economic Forum rated data fraud or theft and cyber-attacks as the fourth and fifth most likely business risks, behind only extreme weather-events, climate change and natural disasters. The COVID-19 pandemic has accelerated our reliance on, and uptake of digital technology as more Australians turn to online platforms and services to manage their businesses, access essential services and engage with their community. Increased reliance on technology means that the economic and social consequences of cyber security incidents is rising.

The Digital Business Plan is part of the Government's economic recovery plan to grow the economy, create jobs and enable Australia to become a leading digital economy and society by 2030. The Digital Business Plan is built on five key pillars, including trust and security. The five pillars identified in the Digital Business Plan reflect the clear role for Government to drive productivity by accelerating the digital transformation of Australian businesses. Government has demonstrated its commitment to build trust and security in the digital economy through its $1.67 billion

investment through the Cyber Security Strategy 2020 and delivery of the critical infrastructure and online harms reforms.

Without a strong foundation of trust, businesses and individuals will hesitate to adopt the technologies necessary to boost productivity and create jobs. The role of trust and security in the Digital Business Plan provides protections for businesses and consumers, boosts business confidence and as a result promotes greater business investments and productivity.