Parliamentary Joint Committee on Law Enforcement

Vaccine related fraud and security risks

August 2021

ISBN 978-1-76093-280-0

Contents

Recommendations

Recommendation 1

2.124 The committee recommends the Department of Home Affairs ensure that the spread of COVID-19 misinformation and disinformation is monitored for extremist content and links to international extremist groups, as well as undertake greater efforts to counter misinformation and disinformation, especially among Aboriginal and Torres Strait Islander communities and culturally and linguistically diverse communities.

Members

Chair

Mr Julian Simmonds MP (from 17.03.2021)	LP, QLD

Deputy Chair

Dr Anne Aly MP	ALP, WA

Members

Senator Alex Antic	LP, SA
Senator Lidia Thorpe	AG, VIC
Mr Garth Hamilton MP (from 23.02.2021)	LNP, QLD
Senator Sue Lines	ALP, WA
Senator Helen Polley	ALP, TAS
Mr Pat Conaghan MP	Nat, NSW
Hon Justine Elliot MP	ALP, NSW
Senator Andrew McLachlan (from 13.05.2021)	LP, SA

Former Members

Mr Craig Kelly MP (to 23.2.2021)
Senator Paul Scarr (to 13.05.2021)

Secretariat

Sean Turner, Committee Secretary (from 11.05.2021)
Pothida Youhorn, A/g Committee Secretary (until 7.05.2021)
Kate Gauthier, Principal Research Officer
Kimberley Balaga, Senior Research Officer
Emmie Shields, Senior Research Officer
Bashir Yousufi, Administrative Officer (from 30.06.2021)
Michaela Keating, Administrative Officer (until 29.06.2021)
Alice Clapham, Administrative Officer (until 23.04.2021)

PO Box 6100
Parliament House
CANBERRA ACT 2600

Telephone: (02) 6277 3419
Email: le.committee@aph.gov.au
Committee web page

Abbreviations

ABF	Australian Border Force
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
AFCCC	Australian Food Cold Chain Council
AFP	Australian Federal Police
AUSTRAC	Australian Transaction Reports and Analysis Centre
CALD	culturally and linguistically diverse
CJLEF	Criminal Justice Law Enforcement Forum
Committee	Parliamentary Joint Committee on Law Enforcement
COVID-19 crime inquiry	COVID-19, criminal activity and law enforcement
Cyber Security Centre	Cyber Security Cooperative Research Centre
DSCMS	digital supply chain management systems
Home Affairs	Department of Home Affairs
JIG	Joint Intelligence Group
Pfizer	Pfizer Australia and New Zealand
Serious Crime Bill	Transport Security Amendment (Serious Crime) Bill 2020
UNODC	United Nations Office on Drugs and Crime
WHO	World Health Organisation

Chapter 1
Background

1.1 The dynamic nature of an international pandemic such as COVID-19 carries inherent security risks for governments, businesses and individuals. These security risks are not only related to direct health and economic impacts, but also include the impacts that can arise from increased vulnerabilities to crimes such as fraud during such times.

1.2 Early in the COVID-19 pandemic, there were significant concerns from governments and health authorities regarding the security and integrity of COVID-19 vaccinations, even before such vaccines had been approved for use. Chief among these concerns was whether organised crime groups would create a market for illicit or fake vaccines, or undertake fraud using peoples' uncertainty or desire for vaccines as the 'bait'. There were additional concerns as to whether anti-vaccination groups may seek to impact the rollout of a COVID-19 vaccination program.

1.3 To investigate these issues, the Parliamentary Joint Committee on Law Enforcement (committee) referred this inquiry on 17 March 2021 to inquire into and report on COVID-19 vaccine related fraud and security risks.[1] This inquiry is intended to focus on the fraud and security risks that specifically arise or relate to COVID-19 vaccinations only, given the committee recently finalised its inquiry into broader crime trends during the pandemic, as outlined in greater detail later in this chapter.

1.4 The types of fraud the committee was concerned would arise, and other issues of interest prompting this inquiry, were:

- phone and internet communications using people's COVID-19 related concerns to conduct fraud;
- illicit vaccines;
- fraudulent vaccination certificates;
- the physical safety of COVID-19 vaccines; and
- Australian Government assistance being given to Pacific nations in relation to the above issues.

1.5 The committee is also concerned with fraudulent information regarding COVID-19 vaccines that is being promoted by various individuals and interest groups, as that misinformation is having a measurable impact on law

[1] Parliamentary Joint Committee on Law Enforcement, *Vaccine related fraud and security risks*, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/VaccineFraud (accessed 21 July 2021).

enforcement. These individual fraud and security issues are discussed in detail in Chapter two.

1.6 The committee's finding to date from this inquiry is that concerns regarding fraud and security risks relating to the vaccination rollout have not yet manifested to the degree some anticipated.

1.7 However, there remain serious ongoing concerns regarding risks of future fraudulent behaviour in relation to vaccination certificates, particularly as there is a gradual normalisation of pre-COVID domestic social and economic activity that will rely on vaccination rates instead of measures such as lockdowns and facemasks, as well as the future resumption of international travel.

1.8 Due to such concerns regarding potential future fraudulent behaviour relating to the COVID-19 vaccination status of individuals, which cannot be properly predicted at this point, the committee has resolved to present its current findings in this interim report, while keeping a watching brief over the issue. A final report is intended to be published by February 2021, when the committee has reviewed the fraud and security risks that may arise if a system for proving vaccination status is rolled out by the Australian Government.

1.9 In addition to the committee's recently completed inquiry into broader crime trends during the pandemic, outlined later in this chapter, the committee is also very conscious that there was a marked increase in online child sexual exploitation during the pandemic. Such exploitation, among the most serious and heinous of all crime types, is being addressed by this committee in another current inquiry: *Law enforcement capabilities in relation to child exploitation*, which was referred on 16 June 2021.[2]

Other relevant inquiry reports

1.10 The broad impacts of the pandemic have already been greatly scrutinised, in particular by the Senate Select Committee on COVID-19. However, inquiries to date have largely focused on the health, social and economic impacts of the pandemic.[3]

1.11 To ensure the security and crime impacts of the pandemic were also properly investigated and better understood, in June 2020 this committee commenced an inquiry into trends and changes in criminal activity related to the pandemic and law enforcement responses (COVID-19 crime inquiry). The committee completed its inquiry and presented its final report in June 2021.[4] That inquiry

---

[2] Parliamentary Joint Committee on Law Enforcement, *Law enforcement capabilities in relation to child exploitation*, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/ChildExploitation (accessed 15 July 2021).

[3] Select Committee on COVID-19, *First interim report*, December 2020.

[4] Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, 21 June 2021.

report comprehensively discussed crime trends—including organised crime and fraud—resulting from the pandemic and the measures taken to combat it.

1.12 As the evidence from that inquiry was largely gathered before Australia's vaccination program was underway, the committee referred this inquiry on 17 March 2021 to 'inquire into and report on vaccine related fraud and security risks'.[5] This inquiry is intended to focus on the fraud and security risks that specifically arise or relate to COVID-19 vaccinations only, and this interim report should be read in conjunction with the report of this committee's COVID-19 crime inquiry. The committee acknowledges that this is a rapidly changing environment, particularly in relation to the issue of proof of vaccination status.

Anticipated fraud and security risks

1.13 Fraud costs victims billions of dollars globally each year. The Australian Competition and Consumer Commission (ACCC) reported Australian losses of over $634 million in 2019, and this amount is expected to rise with the release of 2020 statistics.[6]

1.14 Early in the pandemic, there was a great deal of concern for the security and integrity of COVID-19 vaccines. As outlined in the committee's recent COVID-19 crime report, the United Nations Office on Drugs and Crime (UNODC) 'predicted that COVID-19 vaccines could be exposed to falsification and trafficking.' The COVID-19 crime report also highlighted evidence that organised crime groups 'might also be attracted to producing and selling false or illicitly obtained medical or [personal protective equipment] products, as the penalties for these activities are less severe than those associated with the manufacture and distribution of illicit drugs'.[7]

1.15 Dr John Coyne, an expert in responses to organised crime and drug trafficking, also advised the committee during the COVID-19 crime inquiry that 'law enforcement needs upskilling to achieve an understanding of legitimate flows of pharmaceutical products,' and that while Australia has strong border controls, 'law enforcement may need more resourcing to assist in the investigation of illegitimate vaccines as a priority'.[8]

1.16 However, it must be noted that the majority of evidence received by the committee for the COVID-19 crime inquiry was in July–August 2020. The

---

5 Parliamentary Joint Committee on Law Enforcement, *Vaccine related fraud and security risks*, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/VaccineFraud (accessed 21 July 2021).

6 Associate Professor Cassandra Cross, *Submission 8*, p. 1.

7 Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, p. 20.

8 Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, p. 25.

evidence to this current inquiry was received in April–May 2021, when the landscape regarding COVID-19 vaccinations had significantly shifted.

1.17 Evidence to this inquiry has outlined that the impacts of the pandemic—such as people working from home, being increasingly online and feeling vulnerable and isolated—have increased both individuals' and businesses' susceptibility to fraud. The Cyber Security Cooperative Research Centre (Cyber Security Centre) submitted that COVID-19 has 'dramatically impacted the way we live and work,' and in the 'mass migration to working-from-home conditions, many workers and organisations have found themselves with less-than-optimal cyber security protections and inadequate cyber awareness'.[9]

1.18 The Attorney-General's Department noted that there is an increased risk of fraud during the COVID-19 pandemic, due to the complex and time-critical nature of government responses, and because the vaccination program is relevant to all Australians.[10]

1.19 The committee heard that this vulnerability to fraud is exacerbated by the pharmaceutical and health care sectors working in an increasingly digitised environment, where 'cyber security incidents are becoming more common, from attempts to steal data and intellectual property, to preventing relevant computers or networks from operating'.[11]

1.20 The Department of Home Affairs (Home Affairs) submitted that criminals would take advantage of community concerns regarding the pandemic in their fraud and scam activities. Home Affairs further submitted that the potential for fraud accompanying the release of COVID-19 vaccines could be 'the most significant criminal issue associated with COVID-19 to impact Australia over the next 24 months'.[12]

1.21 The Australian National University, School of Regulation & Global Governance, similarly submitted that crime groups exploit supply shortages and widespread fear of COVID-19 as a general template for fraud and other deceptions, including scamming online government relief measures and payments.[13]

1.22 Fraud is not just an issue for individuals and businesses through the risk of losing money. The Attorney-General's Department submitted that fraud can also undermine the efforts of governments to respond quickly in crisis and emergency response situations, highlighting the need for an effective and swift

---

9 Cyber Security Cooperative Research Centre, *Submission 3*, p. 3.

10 Attorney-General's Department, *Submission 10*, [p. 1].

11 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation, *Submission 6*, p. 3.

12 Department of Home Affairs, *Submission 4*, p. 4. See also Pfizer Australia and New Zealand, *Submission 11*, [p. 1].

13 Australian National University, School of Regulation & Global Governance, *Submission 5*, p. 1.

response to fraud risks from governments. The department also observed that fraud can also 'reduce the public's confidence in genuine communications from governments and health practitioners, potentially leading them to disregard advice about vaccine availability and appointments'.[14]

1.23 The Attorney-General's Department further noted that 'if fraud happens in an uncontrolled manner, it could have significant impacts, such as increasing the cost of the rollout or undermining confidence in the vaccines and Australia's vaccination program'.[15]

1.24 The Cyber Security Centre informed the committee that the ability of cyber criminals to adapt to amorphous environments was shown by the rise of COVID-19 vaccine related cyber threats as nations pivoted to vaccine rollouts, and predicted these 'are likely to escalate, morph and mutate as the pandemic continues and the world becomes ever more digitally interconnected'.[16]

Fraud experienced under pandemic

1.25 The committee's COVID-19 crime inquiry report found there was 'conflicting evidence regarding the extent to which cybercrime activity increased during the COVID-19 pandemic'. For example, Home Affairs stated cybercrime increased modestly, while the Cyber Security Centre stated there had been an exponential rise in cyber activity.[17]

1.26 The Cyber Security Centre submitted similar evidence to this inquiry, that '[i]ndividually and collectively, citizens around the world are now facing a greater volume and range of cyber threats' and that during the first COVID-19 lockdown period in 2020, 'Australia witnessed an exponential rise in cyber activity by malicious cyber actors, with the Australian Cyber Security Centre noting in 2020 they had fielded almost 60,000 reports from Australian individuals and organisations purporting instances of cybercrime'.[18]

1.27 The ACCC received reports of scams related to COVID-19 as early as 27 January 2020, with scammers taking advantage of Australian's fears through phishing, selling false products and other types of scams.[19] The Cyber Security Centre

---

[14] Attorney-General's Department, *Submission 10*, [pp. 1–2].

[15] Attorney-General's Department, *Submission 10*, [p. 1].

[16] Cyber Security Cooperative Research Centre, *Submission 3*, p. 3.

[17] Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, p. 31.

[18] Cyber Security Cooperative Research Centre, *Submission 3*, p. 3.

[19] Australian Competition and Consumer Commission, *Submission 9*, p. 1.

submitted that the ACCC has found 'that since the beginning of the pandemic, there have been more than $9,800,000 AUD in reported losses'.[20]

1.28 However, the committee received evidence to the COVID-19 crime inquiry that increases in fraud have also been driven by issues unrelated to the pandemic. The COVID-19 crime inquiry report quoted the Australian Signals Directorate and Australian Federal Police (AFP) as advising that 'advancement and innovation over the last decade was already leading to increased digital adoption and cyber-attacks…deception, theft, corruption, fraud, blackmail, money-laundering, phishing, and scams were already rising around the world, and the pandemic has only exacerbated this trend'.[21]

1.29 Evidence to this inquiry has suggested that, despite the increased instances of fraud during the pandemic, fraud has thus far tended not to use the vaccination program as a vulnerability point. The ACCC noted it had 'continued to see a substantial volume of COVID-19 themes in scams so far in 2021, but a very limited number relate to vaccinations'. The ACCC submitted the instances of fraud relating to vaccines included:

- Between 1 January 2021 and 9 April 2021, Scamwatch received 793 reports mentioning COVID-19 with $2.4 million in reported losses.
- By comparison, only 58 of these 793 reports mentioned COVID-19 vaccines or vaccinations, with no reported financial losses. Of the 58 reports 6 reporters advised that they gave personal information to the scammer. A further 4 reporters advised that they gave personal information however these reports were all legitimate government or medical centre contacts.[22]

1.30 The ACCC advised that common examples of COVID-19 related scams include:

- text, social media posts and emails with misinformation about the coronavirus;
- investment scams claiming coronavirus has created new opportunities to make money or to invest in COVID-19 vaccinations; and
- survey and research scams offering a reward for participation in research or survey about the vaccine.[23]

1.31 Home Affairs advised that the organised crime threat related to the COVID-19 vaccine rollout was significantly reduced in Australia because of the no-cost nature of the government vaccine program, and submitted that the 'impact of organised criminal activity associated with COVID-19 vaccines in Australia is

---

[20] Cyber Security Cooperative Research Centre, *Submission 3*, p. 5.

[21] Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, pp. 31–32.

[22] Australian Competition and Consumer Commission, *Submission 9*, p. 2.

[23] Australian Competition and Consumer Commission, *Submission 9*, p. 3.

likely to be limited to scam attempts and small-scale black market activity.[24] Home Affairs further advised that international experience suggests that while criminal groups will try to exploit the vaccine rollout, 'this is likely to be on a small or individual scale'.[25]

1.32 The Attorney-General's Department noted that:

> Australia has not seen significant scam and fraud activity related to the COVID-19 vaccination roll-out. This is a positive trend we would like to see continued to maintain confidence in the vaccination program.[26]

1.33 The Northern Territory Government also noted it had not experienced the anticipated levels of fraud, and informed the committee that 'no reports of COVID-related telecommunication or internet fraud have been received in the Territory'.[27]

Government countermeasures for fraud

1.34 The committee was informed of a number of existing initiatives, programs and working groups that address fraud and security risks more broadly, that were also relevant to the kinds of fraud risks that arose as a result of the pandemic. The committee was also informed of instances where those existing programs pivoted to address COVID-19 related risks, or where new programs or taskforces were set up to target COVID-19 specific crimes, including fraud and other criminal activities. The existence of these initiatives, which pre-date the pandemic, is likely a significant contributor to the relatively low rate of COVID-19 related fraud that has, to date, been actually experienced as opposed to anticipated.

1.35 The following section will discuss some pre-existing Australian Government measures to address fraud, and how those measures were already relevant to, or adapted to address, COVID-19 related fraud and security risks. This is not an exhaustive list of all the measures taken by the Australian Government to tackle fraud and cyber security, but is meant to briefly outline some of the key existing measures. New measures introduced specifically to counter COVID-19 related fraud are discussed in chapter two. Some broader measures were also discussed in this committee's report into the COVID-19 crime inquiry.

1.36 The Criminal Justice Law Enforcement Forum (CJLEF) consists of the heads of 17 Commonwealth agencies and was established by Home Affairs in 2017–18, to ensure the agency is 'bringing together the Commonwealth's collective capabilities to bear against capable and well-resourced organised crime

---

[24] Department of Home Affairs, *Submission 4*, p. 2.

[25] Department of Home Affairs, *Submission 4*, p. 2.

[26] Attorney-General's Department, *Submission 10*, [p. 1].

[27] Northern Territory Government, *Submission 1*, p. 1.

syndicates'.[28] Home Affairs submitted that under the pandemic, the CJLEF 'is driving an integrated response to COVID-19 criminality' to 'better coordinate public messaging for greater public confidence in the vaccine program, and reduce opportunities for scam and fraud activity'.[29]

1.37 The Attorney General's Department manages the Commonwealth Fraud Prevention Centre, which has pivoted during the pandemic to undertake work to prevent COVID-19 related crime. The Commonwealth Fraud Prevention Centre, together with the AFP and the Department of Health, assists in the 'design and implementation of Australia's COVID-19 vaccination rollout to provide information about fraud threats identified internationally and discuss strategies to assess and mitigate those threats in Australia'.[30]

1.38 The Attorney-General's Department also informed the committee of broader anti-fraud work being undertaken by that agency to counter fraud risks in the Australian community, which are relevant to fraud experienced during the pandemic:

> A key first step to countering fraud is undertaking fraud risk assessments. A detailed, fraud-focused assessment provides relevant public officials with a better understanding of fraud risks and highlights any limitations in existing countermeasures. A fraud risk assessment also helps officials make decisions about how to mitigate fraud risks and where to focus post-event assurance activities.[31]
>
> [The Attorney-General's Department], through the [Commonwealth Fraud Prevention Centre], has published leading practice guidance on fraud risk assessments on its website, CounterFraud.gov.au. These assessments have evolved significantly over recent years, and can lay the groundwork for additional improvements, such as improved data collection, collaboration, information sharing, data analytics and countermeasures that can be scaled across different measures and programs.[32]

1.39 The Australian Cyber Security Centre is based within the Australian Signals Directorate and leads the Australian Government's efforts to improve cyber security. It provides advice and information about how to protect individuals and businesses online, works collaboratively to investigate and develop solutions to cyber security threats and works with law enforcement authorities to fight cybercrime.[33]

---

28 Department of Home Affairs, *Annual Report 2017–18*, p. 15.

29 Department of Home Affairs, *Submission 4*, p. 5.

30 Attorney-General's Department, *Submission 10*, [pp. 1 and 3].

31 Attorney-General's Department, *Submission 10*, [p. 3].

32 Attorney-General's Department, *Submission 10*, [p. 3].

33 Australian Cyber Security Centre, *About the ACSC*, www.cyber.gov.au/acsc (accessed 15 July 2021).

1.40 Working closely with the Australian Cyber Security Centre, the Department of Health is undertaking measures to deal with vaccine fraud risks, including potential cyber issues. The Therapeutic Goods Administration has also been working on measures to mitigate the risk of counterfeit vaccines.[34]

1.41 Home Affairs is the lead agency responsible for implementing Australia's recently announced *Cyber Security Strategy 2020*, and is 'developing a new national framework on measures to detect, deter, prevent, respond and recover from the harms caused by both cyber-dependent and cyber-enabled cybercrime' and is also exploring new opportunities for collaboration with the National Australia Bank via a new working group.[35]

1.42 Home Affairs informed the committee that initiatives developed under this broader cyber security program will be relevant to COVID-19 related crime but were not created to address only the crimes that arose under the pandemic.[36]

1.43 One Home Affairs initiative is the national identity-matching services, including the Document Verification Service and Face Matching Services, which provide a fast, secure, online check of identity information against government identity records, which is a valuable tool in combatting identity fraud.[37]

1.44 Home Affairs noted the Identity-matching Services Bill 2019 will make driver's licence images matchable for the first time, improving the capability of the Commonwealth, State and Territory agencies to share identity information for verification and identification purposes in support of fraud prevention, law enforcement, national security, and service delivery outcomes.[38] This bill is currently before Parliament.[39]

1.45 Additionally, Home Affairs has engaged IDCARE to 'ensure Australian victims of identity scams and cyber-crimes have the specialist support they need to recover from and minimise the impact of these incidents'.[40]

1.46 The AFP advised that under the *Cyber Security Strategy 2020*, it had been funded for $89.9 million in relation to cybercrime, and also discussed the new collaboration with the National Australia Bank 'to help us identify the scope and

---

34 Attorney-General's Department, *Submission 10*, [pp. 1 and 3].

35 Department of Home Affairs, *Submission 4*, p. 4.

36 Department of Home Affairs, *Submission 4*, p. 4.

37 Department of Home Affairs, *Submission 4*, p. 4.

38 Department of Home Affairs, *Submission 4*, p. 4.

39 The bill was reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), which recommended amendments to the bill. See PJCIS, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019*, October 2019.

40 Department of Home Affairs, *Submission 4*, p. 4.

scale of what they're seeing' and described it as 'a really fruitful partnership for us, not just a relationship'.[41]

1.47 The AFP has a range of other measures that are relevant to COVID-19 related crimes. Operation Ashiba is an AFP-led multi-agency taskforce 'established to support and contribute to whole-of-government efforts to combat serious and organised crime exploiting Commonwealth funded programs'.[42] Operation Ashiba now auspices the temporary COVID-19 Counter Fraud Taskforce that focuses on fraud against COVID-19 economic stimulus measures.[43]

1.48 To progress goals of the COVID-19 Counter Fraud Taskforce, the AFP established Taskforce Iris, comprised of two dedicated investigation strike teams in Melbourne and Sydney, with additional investigations teams to provide support across the country as needed.[44]

1.49 In March 2020, the AFP established Operation PROTECT to coordinate the AFP's involvement in the whole-of-government response to the pandemic, with a 24/7 Incident Coordination Centre located at AFP Headquarters in Canberra and Major Incident Rooms in all AFP regional offices.[45]

1.50 In the same month, the AFP also established the Joint Intelligence Group (JIG) as the central point of intelligence for Operation PROTECT. The JIG monitors and shares information on crime trends and potential risks among its members, which includes international partners and Australian law enforcement and intelligence agencies, such as Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Criminal Intelligence Commission (ACIC) and Australian Border Force (ABF) and all state and territory police forces.[46]

1.51 The ACCC's Scamwatch service has monitored scams throughout the pandemic. The service allows consumers to report scams, which the ACCC then monitors

---

41 Commissioner Reece Kershaw, Commissioner, Australian Federal Police, *Committee Hansard*, 12 April 2020, pp. 4–5.

42 Australian Federal Police, *Operation Ashiba – Basic Facts*, June 2020, p. 1.

43 Attorney-General's Department, *Counter fraud during the COVID-19 pandemic*, www.ag.gov.au/integrity/counter-fraud/counter-fraud-during-covid-19-pandemic (accessed 16 July 2021).

44 Commonwealth Fraud Prevention Centre, *Operation Ashiba and Taskforce Iris – Strengthening Australia's response to serious and organised fraud*, www.counterfraud.gov.au/news/general-news/operation-ashiba-and-taskforce-iris-strengthening-australias-response-serious-and-organised-fraud (accessed 16 July 2021).

45 Australian Federal Police, *Submission to the Parliamentary Joint Committee inquiry into COVID-19, criminal activity and law enforcement*, p. 2.

46 Australian Federal Police, *Submission to the Parliamentary Joint Committee inquiry into COVID-19, criminal activity and law enforcement*, pp. 2–3.

to understand and raise public awareness of scams trends. The ACCC also undertakes intelligence sharing and disruption activities.[47]

1.52 International collaborative groups have also pivoted to address COVID-19 related risks. Via the International Public Sector Fraud Forum, the Attorney-General's Department has shared information on fraud threats and incidents during the COVID-19 pandemic response with international counterparts from the UK, US, New Zealand and Canada, as well as leading counter fraud approaches.[48]

1.53 Chapter two will discuss new measures introduced specifically to counter COVID-19 related fraud, focused only on the measures that are relevant to vaccine related fraud.

Conduct of this inquiry

1.54 The committee referred this inquiry on 17 March 2021 into vaccine related fraud and security risks, pursuant to subsection 7(1) of the *Parliamentary Joint Committee on Law Enforcement Act 2010*.

1.55 The terms of reference for the inquiry required the committee to inquire into and report on vaccine related fraud and security risks, with particular reference to:

(a) Telecommunications and internet fraud relating to COVID vaccinations;
(b) Criminal activity around the supply of fake vaccines, black market vaccines and/or fake vaccine certifications and the acquisition of certificates;
(c) Risks to Australia regarding fraud and integrity of COVID vaccines in South Pacific nations and support for these nations to address issues relating to fraud and integrity risks;
(d) Physical security in the production, transport and supply of COVID vaccines in Australia;
(e) Measures to prevent and protect against COVID vaccine-related fraud and security risks;
(f) Any related matters.[49]

1.56 The committee received 14 submissions. A list of public submissions, together with other information authorised for publication is provided at Appendix 1.

1.57 The committee has not held a public hearing for this inquiry prior to publishing this interim report.

---

47 Australian Competition and Consumer Commission, *Submission 9*, p. 1.

48 Attorney-General's Department, *Submission 10*, [p. 2].

49 Parliamentary Joint Committee on Law Enforcement, *Vaccine related fraud and security risks, Terms of Reference*, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/VaccineFraud/Terms_of_Reference (accessed 21 July 2021).

Public hearing

1.58 The evidence submitted from law enforcement agencies advised that, on the whole, the anticipated spike in fraud connected to the COVID-19 vaccine rollout has not, at least to date, occurred in Australia. As such, the committee did not hold public hearings to assist in drafting this interim report. However, public hearings may be held at a future date to seek further evidence for the final report of this inquiry.

Acknowledgements

1.59 The committee thanks the individuals and organisations that made submissions to the inquiry to date.

Final report

1.60 As noted earlier in this chapter, a final report is intended to be published by February 2022, after the committee has reviewed the fraud and security risks that may arise if a system for proving vaccination status is rolled out by the Australian Government.

Chapter 2
Vaccine fraud risks

2.1 Chapter one outlined some of the key ongoing measures taken by Australian Government agencies to counter fraud that pre-date the COVID-19 pandemic. Chapter one also outlined how those pre-existing efforts were pivoted to address new fraud methods that emerged during the pandemic, many of which include measures that will address crimes relating to COVID-19 vaccines.

2.2 This chapter will discuss fraud and security risks that are specific to COVID-19 vaccines, and new law enforcement responses to those risks. Because these law enforcement efforts address multiple crime types, this chapter will first outline the law enforcement efforts to protect the integrity and security of COVID-19 vaccines as a whole, before discussing some of the key individual fraud and security risks that relate to COVID-19 vaccines.

Whole of issue countermeasures

2.3 The committee was informed that Australian Government agencies are working collaboratively in cross-portfolio efforts to identify and address risks to society related to the COVID-19 vaccination program, including the health, social, economic and security impacts.[1] Multiple agencies are actively monitoring potential criminal threats related to the COVID-19 pandemic, including 'attempted import of illicit vaccines, criminality in the supply chain, and fraud and scam activity relating to the vaccine rollout, including fraud at the point of vaccination'.[2]

2.4 The Attorney-General's Department submitted:

> There are risks inherent in any large scale activity – particularly one as complex as delivering a national vaccination program as quickly as possible. The best way to prevent risks from being realised is to identify them early and determine appropriate treatments, where possible.[3]

2.5 On 8 February 2021, the Australian Federal Police (AFP) created Taskforce LOTUS to respond to criminal acts related to the rollout of the COVID-19 vaccine in Australia. The early establishment of the taskforce before the vaccine rollout commenced was planned to allow for quick operational responses, and via this taskforce the AFP will be able to assist Commonwealth partners should the need arise to investigate COVID-19 vaccine related crimes ranging from 'the

---

1 Department of Home Affairs, *Submission 4*, p. 2. See also Attorney-General's Department, *Submission 10*, [pp. 1 and 3–5] and Department of Health, *Submission 14*, p. 12.

2 Department of Home Affairs, *Submission 4*, p. 2.

3 Attorney-General's Department, *Submission 10*, [p. 3].

mass theft of vaccines through to fraud-related scams against Commonwealth procurements and grants'.[4]

2.6 The AFP also deployed personnel across the country under Operation PROTECT, to support state and territory police in response to the pandemic. AFP Commissioner Reece Kershaw stated this 'demonstrates our commitment to protecting vulnerable communities in the north and protecting Australia's borders'.[5]

2.7 As outlined in Chapter one, the widespread distribution of no cost COVID-19 vaccines mitigates the organised crime threat in Australia, with the most likely remaining threats limited to scam attempts and small-scale black-market activity. However, even while minimal, there have been some fraud and security risks directly linked to COVID-19 vaccines. These issues are discussed below.

Telephone and internet fraud

2.8 The development and increased use of communications technologies has enabled fraud offenders to engage with a larger pool of potential victims in ways that are cheaper and easier than using older methods of communication. Associate Professor Cassandra Cross, an expert in cybercrime, advised that while a large proportion of fraud is conducted online, offenders still use telephone, fax and face-to-face methods:

> My own research demonstrates the ways in which offenders will move seamlessly across all communications platforms (including email, telephone, text message, social media and face-to-face) to perpetrate their offences.[6]

2.9 In relation to the changing fraud threat during the COVID-19 pandemic, the committee heard that a significant proportion of COVID-19 related crime will be where criminals use vaccine-themed telephone and online phishing[7] scams to obtain personal identification information to exploit for future fraud, with cyber criminals 'preying on citizens' anxieties and uncertainties, along with less secure [working from home] conditions to take advantage of the COVID-19 vaccine rollout through online scams.[8]

---

4 Department of Home Affairs, *Submission 4*, p. 3.

5 Commissioner Reece Kershaw, Commissioner, Australian Federal Police, *Committee Hansard*, 12 April 2021, p. 2.

6 Associate Professor Cassandra Cross, *Submission 8*, p. 1.

7 Phishing is where an attacker sends a fraudulent message designed to trick a victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure.

8 Cyber Security Cooperative Research Centre, *Submission 3*, p. 5 and Department of Home Affairs, *Submission 4*, p. 4. See also Australian Competition and Consumer Commission, *Submission 9*, p. 1, Commissioner Reece Kershaw, Australian Federal Police, *Committee Hansard*, 12 April 2020, p. 2.

2.10 Associate Professor Cross similarly advised that as anxiety levels have understandably increased during the pandemic, offenders have taken advantage of this anxiety, 'as well as the corresponding factors related to COVID-19 and all government measures put in place since March 2020' in order to commit crime.[9]

2.11 Associate Professor Cross further advised that there is a 'well-established link between natural disasters and fraud, with offenders using these events in a variety of ways to gain their monetary benefits'. As such, the use of COVID-19 for fraudulent purposes is 'consistent with previous research'.[10]

2.12 The Australian Competition and Consumer Commission's (ACCC) Scamwatch has warned of online scams related to COVID-19 vaccinations in Australia, with the most prevalent being:

- requesting payment for vaccines or for early access to vaccines;
- offers to mail vaccines;
- offers to pay money as an investment opportunity in the Pfizer vaccine;
- fake surveys related to vaccines that offer prizes or early access.[11]

2.13 The Department of Home Affairs (Home Affairs) outlined that cyber criminals would likely target cohorts identified as priority vaccine recipients, which is of concern as elderly people have a heightened vulnerability to scam activity.[12]

2.14 The committee was also advised that cyber criminals will often masquerade as legitimate organisations such as the World Health Organisation (WHO), which had to issue a warning that 'that hackers and cyber scammers have been impersonating the organisation by sending emails and WhatsApp messages containing malicious links'.[13]

2.15 The Attorney-General's Department advised that changes to Australia's vaccination program, such as the changes in age-limits associated with the AstraZeneca vaccine, provides additional opportunities for fraudsters to take advantage of public uncertainty and successfully scam individuals and organisations.[14]

2.16 Professor Cassandra Cross similarly submitted that while the development and release of an approved vaccine 'was an historic moment', it 'also provided

---

9 Associate Professor Cassandra Cross, *Submission 8*, p. 3.

10 Associate Professor Cassandra Cross, *Submission 8*, p. 3.

11 Cyber Security Cooperative Research Centre, *Submission 3*, pp. 3, 5–6.

12 Department of Home Affairs, *Submission 4*, p. 4.

13 Cyber Security Cooperative Research Centre, *Submission 3*, p. 3.

14 Attorney-General's Department, *Submission 10*, [p. 2].

additional opportunities for offenders to embrace the pandemic and virus as a means to extend their fraudulent pitches'.[15]

2.17 Home Affairs identified that cyber criminals may seek to acquire sensitive personal identification information such as Medicare and MyGov information by impersonating health services. This can then be on-sold to be exploited for future fraudulent activity including 'banking and credit card fraud, superannuation fraud, tax fraud, Medicare fraud, and Centrelink fraud.[16]

2.18 Instances of fraud using medicines as bait experienced during the pandemic have not been limited to those offering fraudulent access to COVID-19 vaccines. As many people are unable or unwilling to shop in person, the increase in online shopping has seen a corresponding rise in online shopping fraud, where 'offenders have created fake websites and social media pages to advertise for products that do not exist'.[17]

2.19 In addition to individuals being targeted for fraud, there has been the additional threat of 'ransomware' attacks on organisations involved in Australia's COVID-19 supply chain, which could disrupt the COVID-19 vaccine rollout.[18]

2.20 However, as outlined in Chapter one, the actual levels of pandemic-related fraud experienced by Australians has to date been less than expected. This has been particularly true in relation to vaccines, largely due to the no-cost public health nature of Australia's COVID-19 vaccination program.

Responses to fraud threats

2.21 As outlined in Chapter one, the Australian Government, via a broad range of agencies with differing skillsets and focus, has a comprehensive network of initiatives to tackle fraud in the Australian community, and many of those initiatives were either already relevant to fraud risks under the pandemic, or were quickly re-focused to become more relevant.

2.22 In regards to crime that specifically relates to COVID-19 vaccines, Home Affairs informed the committee that the Joint Intelligence Group (JIG), as outlined in Chapter one, is able to leverage the collective intelligence assessment of the national intelligence community and international stakeholders, with a 'dedicated analytic focus and an inter-agency group to inform on specific threats

---

[15] Associate Professor Cassandra Cross, *Submission 8*, p. 4.

[16] Department of Home Affairs, *Submission 4*, p. 4. See also Associate Professor Cassandra Cross, *Submission 8*, p. 3.

[17] Associate Professor Cassandra Cross, *Submission 8*, p. 3.

[18] Department of Home Affairs, *Submission 4*, p. 4.

including: the facilitation and legitimate trade of approved COVID-19 vaccine imports; and illegitimate trade of COVID-19 vaccines'.[19]

2.23 In addition to the fraud countermeasures already discussed, the Australian Communications and Media Authority submitted it continues to publish warnings for 'all Australians to remain in a state of heightened alert to email and SMS scams that seek to trick people into giving out personal data in exchange for (false) vaccine bookings,' and the ACCC's Scamwatch has built a specialist COVID-19 scam portal highlighting all current coronavirus-related scams.[20]

2.24 However, the Cyber Security Cooperative Research Centre (Cyber Security Centre) has submitted that while these public messaging initiatives are commendable, 'more can be done to ensure complacency does not develop across the population and to ensure the public is advised, in real-time, of new threats and challenges'.[21]

Illicit vaccines and certificates

2.25 A concern of law enforcement agencies at the start of the pandemic, was whether there would be an Australian market for illicit or fake vaccines. Illicit vaccines include counterfeit, fake or unviable vaccines, as well as genuine vaccines obtained outside the approved Australian health system which could be diverted from overseas or domestic supply chains.[22]

2.26 The Cyber Security Centre submitted that 'Australia may prove to be particularly vulnerable to illegal COVID-19 black markets, with one of the world's highest concentrations of darknet drug vendors per capita'.[23]

2.27 The Attorney-General's Department advised that suppliers could seek to sell or administer vaccines that have not been stored properly, and there was also the risk of vaccines being deliberately tampered with before being administered, rendering them no longer effective, putting the public at risk and potentially undermining public confidence in the vaccine.[24]

2.28 Pfizer Australia and New Zealand advised the committee that illicit or counterfeit products pose risks to health for individuals. The danger can lie in sophisticated counterfeit products that are difficult to identify, even for healthcare professionals.[25] Home Affairs similarly submitted that it is possible

---

19 Department of Home Affairs, *Submission 4*, p. 3.

20 Cyber Security Cooperative Research Centre, *Submission 3*, p. 5.

21 Cyber Security Cooperative Research Centre, *Submission 3*, p. 6.

22 Department of Home Affairs, *Submission 4*, p. 2.

23 Cyber Security Cooperative Research Centre, *Submission 3*, p. 7.

24 Attorney-General's Department, *Submission 10*, [p. 3].

25 Pfizer Australia and New Zealand, *Submission 11*, [p. 1].

that some individuals or groups would try to acquire specific brands or fast-track their own vaccination.[26]

2.29 Pfizer Australia and New Zealand argued that this risk made it essential that all COVID-19 vaccines and treatments are obtained from legal and authorised distributors.[27] Home Affairs submitted that this risk has been successfully managed by the free vaccine rollout in Australia, which minimises 'demand from Australians seeking vaccines for their own supply'.[28]

2.30 There is an additional risk whereby criminals may seek to illegally refill empty vaccine vials for sale, but the strict procedures for vaccine vial disposal has mitigated this risk.[29]

2.31 The Cyber Security Centre advised that it is vital to 'amplify public messaging advising all Australians that vaccines are not available for private sale' to counter the risk of people being exposed to fake or illicit vaccines.[30]

2.32 Another area of concern was the risk of fraudulent or counterfeit vaccination certificates. The Attorney-General's Department has identified vaccine certificate fraud as a potential fraud risk, and submitted:

> Fraud risk assessments should be complemented by ongoing monitoring of risks to ensure officials stay alert to the changing nature of the fraud threat, and manage the evolving risk accordingly. For example, as international borders reopen, new threats will emerge such as the sale and use of counterfeit vaccine certificates, which could risk public safety and undermine efforts to restore Australia's tourism sector.[31]

2.33 However, since the time of the above submission, proof of vaccination status is an emerging issue that is no longer only relevant to international travel, but may also be utilised within Australia for some workplaces or accessing certain services. The law enforcement risks associated with fraudulent vaccination certificates are discussed in greater detail later in this chapter.

Responses to fake vaccine risks

2.34 Home Affairs informed the committee that, in addition to ongoing border protection efforts, it contributes to whole-of-government efforts to protect the integrity of the COVID-19 vaccination rollout through 'securing the supply

---

[26] Department of Home Affairs, *Submission 4*, p. 2.

[27] Pfizer Australia and New Zealand, *Submission 11*, [p. 1].

[28] Department of Home Affairs, *Submission 4*, p. 2.

[29] Department of Home Affairs, *Submission 4*, p. 2.

[30] Cyber Security Cooperative Research Centre, *Submission 3*, p. 7.

[31] Attorney-General's Department, *Submission 10*, [p. 4].

chain, while ensuring border controls remain effective in identifying and intercepting fake, counterfeit and diverted vaccines'.[32]

2.35 Home Affairs has reported that as of 30 April 2021, no illicit vaccines had been detected at Australia's borders. However, the agency also noted that attempted imports may increase as the availability of vaccines globally also increases.[33]

2.36 Home Affairs further informed the committee that importations are being closely monitored to 'identify and disrupt any criminal actor seeking to exploit vulnerabilities in the vaccine program through illegitimate importation'. However, it was further noted that should this threat eventuate, 'it will likely be small scale and demand driven by individuals who may attempt to import vaccines into Australia'.[34]

Physical security of COVID-19 vaccines

2.37 This section will review the physical security aspects of the production, transport and supply of COVID-19 vaccines. The supply chains of COVID-19 vaccines in Australia are of significant importance in the successful rollout of the vaccination program, and can ultimately impact the success of ending the pandemic.

2.38 Deakin University (Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation) noted there is an 'increasingly globalized vaccine supply chain' where 'risks relating to the provenance, authenticity and integrity of the vaccines may cause cascading failure and have devastating consequences'. Furthermore, Deakin University noted that 'the issues around the COVID pandemic have changed the vaccine supply chain's importance and significance, given the "large scale nature" of the activity'.[35]

2.39 The supply chain in Australia for COVID-19 vaccines has two key vulnerabilities, the first being the challenge of meeting the storage temperature requirements, often referred to as a 'cold chain'. The second vulnerability is physical security, where malicious or criminal actors may seek to steal or tamper with vaccines. These vulnerabilities are discussed below.

Cold chain vulnerabilities

2.40 The Australian Food Cold Chain Council (AFCCC) provided the committee with a definition of a cold chain:

---

[32] Department of Home Affairs, *Submission 4*, p. 2.

[33] Department of Home Affairs, *Submission 4*, p. 2.

[34] Department of Home Affairs, *Submission 4*, p. 2.

[35] Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation, *Submission 6*, p. 4.

> The cold chain is a temperature-controlled supply chain of separate refrigerated events sufficient to achieve continuous temperature control of perishable goods. An unbroken, or compliant cold chain is an uninterrupted series of these events used to store and transport perishable products from one destination to another.[36]

2.41 Unbroken cold chains are particularly relevant for vaccines, as vaccines require specific storage, transportation and equipment to administer effectively.[37] The Pfizer vaccine needs to be kept at freezer temperatures for up to two weeks during transport, and at regular fridge temperatures for up to five days.[38]

2.42 Deakin University noted, 'the COVID pandemic has already highlighted the lack of resilience in many supply chains, as supply chain networks fail from disruptions at single nodes and connections'.[39]

2.43 The AFCCC made a submission providing substantive comment on cold chain vulnerabilities in Australia, informing the committee that there are 'very few compliant end-to-end cold chains in Australia', primarily due to long distances, commercial pressures and multiple use of third party logistics providers. The AFCCC raised further concerns that a lack of understanding about how to assess cold chain compliance meant this problem may, in fact, be far greater than initially assessed, and is growing with the increased use of electronic data from telematics devices in storage and transport assets.[40]

2.44 The AFCCC raised concerns specific to vaccine transport:

> Unfortunately, it is common practice in Australian pharmaceutical delivery to use a mixture of temperature-controlled packages, thermal boxes or packages with or without temperature measurement, and hardly ever with temperature monitoring. Transport assets in Australia are usually not validated or tested for pharmaceutical transport, and transporters have no systems in place to adequately verify temperature at the CCP or delivery.[41]

2.45 The AFCCC advised there is significant work to be done to improve the Australian cold chain, and made a number of specific recommendations relating to temperature verification, standards for transport assets and door monitoring.[42]

---

36 Australian Food Cold Chain Council, *Submission 2*, p. 2.

37 Attorney-General's Department, *Submission 10*, [p. 3].

38 Cyber Security Cooperative Research Centre, *Submission 3*, p. 10.

39 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation (Deakin University), *Submission 6*, p. 4.

40 Australian Food Cold Chain Council, *Submission 2*, p. 3.

41 Australian Food Cold Chain Council, *Submission 2*, p. 4.

42 Australian Food Cold Chain Council, *Submission 2*, pp. 5–6.

Physical security of vaccines

2.46 The committee was told of a number of vulnerabilities in the physical security of COVID-19 vaccines, some of which can manifest via cyber activity.

2.47 Deakin University submitted that nearly 80 per cent of vaccine manufacturers consider it important to increase the focus on tracking and tracing along vaccine supply chains, and noted that 'large pharmaceutical companies involved in the production of COVID vaccines are no stranger to safety and security risks and cyber-espionage'.[43] Deakin University advised that 'proactively tracking and tracing along the vaccine supply chains will increase the probability that vaccination programs meet their goals,' and questioned whether a vaccination program would prove viable without efficient tracking and tracing.[44]

2.48 Home Affairs submitted that it was possible that 'individuals and organised crime groups may attempt to exploit handling, shipping and storage measures to steal or divert legitimate vaccines from Australia's supply chain to sell on the domestic black market or for illicit export'.[45]

2.49 The Attorney-General's Department similarly submitted that there are a number of links in the vaccine supply chain that are vulnerable to fraud, theft or tampering, and changes during the rollout could create further vulnerabilities.[46]

2.50 In May 2020, the Department of Foreign Affairs and Trade noted that malicious cyber activity was targeting hospitals, medical services and crisis response organisations outside of Australia.[47]

2.51 While the above malicious activity is conducted online, the Cyber Security Centre submitted that cyber attacks are a threat to physical storage locations of vaccines at medical facilities and noted that in July 2020 'it was disclosed that state-based cyber actors from Russia and North Korea had targeted vaccine production facilities with cyber attacks'. In that instance, the cyber attack resulted in the shutdown of the COVID-19 vaccine manufacturing facilities.[48]

2.52 The Northern Territory Government informed the committee that it recently completed a security review at major hospitals and would act upon any recommendations arising out of that audit.[49]

---

43 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation, *Submission 6*, p. 4.

44 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation, *Submission 6*, p. 4.

45 Department of Home Affairs, *Submission 4*, p. 2.

46 Attorney-General's Department, *Submission 10*, [p. 3].

47 Cyber Security Cooperative Research Centre, *Submission 3*, p. 3.

48 Cyber Security Cooperative Research Centre, *Submission 3*, p. 10.

49 Northern Territory Government, *Submission 1*, p. 1.

Responses to physical security threats

2.53 The committee received evidence of a range of activities being undertaken to ensure a whole-of-government response to ensure the physical security of COVID-19 vaccines. Much of this response is discussed in the earlier section on whole-of-issue countermeasures. The following section will discuss some activities that only relate to physical security.

2.54 Home Affairs informed the committee that a joint operation supported the Australian Government's efforts to facilitate legitimate COVID-19 vaccines into the border, including the Australian Border Force (ABF) contribution to the logistics network design for the movement of vaccine products, facilitated and implemented by the Department of Health. ABF's border processes 'will enable legitimate vaccines to be identified pre-border and give expedited border clearance through to a secure domestic distribution network managed by the Department of Health'.[50]

2.55 Home Affairs submitted that the ABF response is informed by regular engagement with 'key industry bodies and international partners, contemporary intelligence, law enforcement and whole-of-government partners, and the experience of key stakeholders'. Home Affairs submitted this approach helps identify supply chain vulnerabilities and allows the ABF to implement an effective, multidisciplinary response to ensure the supply chain integrity of Australia's COVID-19 vaccine supply.[51]

2.56 Additionally, ABF officers have received specialised training by vaccine manufacturers to assist them to identify potential illegitimate vaccines, and the ABF, AFP and Therapeutic Goods Administration are collaboratively sharing information and intelligence in relation to counterfeit and unapproved therapeutic goods.[52]

2.57 Home Affairs further informed the committee that it was working in partnership with the ABF in threat assessment of trusted insiders across the vaccine supply chain, and stated it will continue to work across Government to ensure adequate risk controls remain in place for the secure transport of COVID-19 vaccine products.[53]

2.58 Home Affairs also outlined an operation, STOP II, conducted by the World Customs Organisation, which commenced 1 April 2021 and involves the intelligence-led targeting of cargo suspected of containing COVID-19 related illicit goods, with a particular focus on counterfeit vaccines. The ABF is

---

50 Department of Home Affairs, *Submission 4*, pp. 2–3.

51 Department of Home Affairs, *Submission 4*, p. 3.

52 Department of Home Affairs, *Submission 4*, p. 3.

53 Department of Home Affairs, *Submission 4*, p. 3.

participating in the operation, which involves up to 183 partner agencies globally.[54]

2.59 Deakin University pointed to advice from the World Bank that digital supply chain management systems (DSCMS) 'can offer a series of benefits and support the supply chains for COVID vaccines'. Such systems would include batches of vaccines serialised for easy identification, proof of pick-up and delivery confirmed via an authenticated chain of custody, and reporting through DSCMS.[55]

2.60 Pfizer Australia and New Zealand (Pfizer) submitted the processes it undertakes to ensure robust systems are in place to help preserve the security of the Pfizer-BioNTech COVID-19 vaccine. Pfizer advised it continued to:

- Maintain key partnerships with anti-counterfeiting coalitions and Law Enforcement around the world to identify and refer cases to the appropriate law enforcement entity.
- Leverage detailed logistical plans and tools to support effective Vaccine transport, storage and continuous temperature monitoring.
- Ship multi-dose vials of the Pfizer-BioNTech COVID-19 Vaccine in specially designed, fit for purpose packaging with robust security features such as GPS-enabled thermal sensors with a dedicated Pfizer control tower that tracks the location and real-time temperature of each Vaccine shipment across its pre-set routes.
- Perform security assessments of key manufacturing and distribution locations and processes, and use specific transportation partners to ship the Vaccine by air to major hubs within a country/region and by ground transport to dosing locations.
- Work closely with distributors to ensure vaccines are safe, including providing a Pfizer Security Liaison.[56]

54 Department of Home Affairs, *Submission 4*, p. 3.

55 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation (Deakin University), *Submission 6*, p. 5.

56 Pfizer Australia and New Zealand, *Submission 11*, [p. 2].

Proposed legislative changes

2.61 Home Affairs noted that provisions in the Transport Security Amendment (Serious Crime) Bill 2020 (Serious Crime Bill) that is currently before the Senate would address a key supply chain vulnerability by ensuring that only the most trusted individuals have unescorted access to secure areas at airports and seaports. Currently, serious and organised crime groups attempt to recruit trusted insiders who have access to the most secure and vulnerable areas of airports and seaports. The Serious Crime Bill would 'assist in combatting serious criminal influence at security controlled airports and seaports by introducing expanded eligibility criteria that must be met by applicants and holders of aviation and maritime security identification cards'.[57]

2.62 The Cyber Security Centre advised that another proposed legislative change, the Security Legislation Amendment (Critical Infrastructure) Bill 2020, 'will assist in bolstering the cyber posture of Australia's critical infrastructure' as it expands the defined critical infrastructure sectors from four to eleven, and would include the health care and medical sector and transport.[58]

Vaccination certificates

2.63 The Department of Health advises that higher vaccination rates make COVID-19 outbreaks much less likely, and therefore reduces the need for preventive measures such as border closures and travel restrictions, subsequently reducing the health, social and economic impacts of the COVID-19 pandemic.[59]

2.64 The issue of whether people need to prove their vaccination status via vaccination certificates is an emerging health policy issue in Australia, which could have law enforcement impacts should people seek to create or use fraudulent documents. Proof of vaccination status is becoming more relevant as greater proportions of the population are vaccinated and governments seek to move away from lockdowns and similar measures, and instead look to vaccination rates as being the key defence against further outbreaks of coronavirus.

2.65 Prime Minister, the Hon. Scott Morrison MP, has indicated that while a COVID-19 vaccination is not likely to be made mandatory,[60] there may be incentives available only to fully vaccinated people, such as entering cafes and pubs,

---

57 Department of Home Affairs, *Submission 4*, p. 3.

58 Cyber Security Cooperative Research Centre, *Submission 3*, p. 11.

59 Department of Health, *Why should I get vaccinated for COVID-19?*, www.health.gov.au/ initiatives-and-programs/covid-19-vaccines/getting-vaccinated-for-covid-19/why-should-i-get-vaccinated-for-covid-19 (accessed 29 July 2021).

60 It should be noted that COVID-19 vaccinations are mandatory for aged care workers, starting 17 September 2021.

because 'if you're vaccinated, you're less of a public health risk than…someone who's unvaccinated'.[61]

2.66 People can currently download and show their vaccination status, including for COVID-19, via the Express Plus Medicare application or a Medicare account. People who are fully vaccinated against coronavirus can download a COVID-19 digital certificate. While there is currently no widespread need to prove COVID-19 vaccination status, future options could include a vaccine certificate being required under pandemic conditions to access certain venues or services, or for travel.[62]

2.67 The Digital Health Agency has recently put out a tender for a 'digital health' smartphone app that will store digital vaccination certificates along with the results of COVID-19 tests and will be available for both Apple iPhone and Google Android devices before December 2021. The app will include 'multiple authenticity and anti-fraud measures'[63]

2.68 However, this approach does entail some risk. Associate Professor Cassandra Cross submitted:

> As more of the population receives their vaccinations, and international borders open for less restricted travel, it is likely that offenders will continue to evolve their approaches accordingly. If vaccination is mandatory in a particular situation (such as travel), this will provide opportunities for offenders to create fake certificates or verification methods. Again, this will be a global issue, and impact countries including Australia.[64]

2.69 The committee has determined that current findings of this inquiry will be published in this interim report, to allow a final report to focus on risks of fraudulent behaviour in relation to proving vaccination status, both domestically and from international arrivals.

South Pacific

2.70 The Cyber Security Centre stressed the importance of Australia's efforts in the Pacific to address needs relating to COVID-19, submitting that:

> [The] unequal distribution of vaccines across socioeconomic demographics of society and between wealthier and less developed countries…introduces

---

61 Charis Chang, 'ScoMo's candid answer about unvaccinated Australians', *News.com.au*, 30 July 2021, www.news.com.au/lifestyle/health/health-problems/scomos-candid-answer-about-unvaccinated-australians/news-story/56abec669500b1a61bc1d21fb550565c (accessed 30 July 2021).

62 Fia Walsh, 'COVID-19 digital vaccination certificates are here. This is what you need to know', ABC Radio Melbourne, 14 June 2021, www.abc.net.au/news/2021-06-13/what-is-a-covid-19-digital-certificate/100205908 (accessed 29 July 2021).

63 David Flynn, 'Australian "vaccination passport" coming to Apple Wallet', *Executive Traveller*, 22 July 2021, www.executivetraveller.com/news/australian-vaccination-passport-coming-to-apple-wallet (accessed 29 July 2021).

64 Associate Professor Cassandra Cross, *Submission 8*, p. 4.

> the very real risk of corruption in the manufacture, allocation and distribution of vaccines.[65]

2.71 The Cyber Security Centre submitted that this inequality 'is a contributing factor to the growing black market for fake vaccines'.[66] To address these concerns, as outlined above, the Australian Government has pledged $80 million to improve vaccine access for Pacific and Southeast Asian countries.

2.72 The Cyber Security Centre advised that 'Australia has a significant role to play in assisting regional partners both during and after the pandemic', and noted this would include assistance for 'both cyber security challenges and support concerning any issues of fraud and integrity risks related to the COVID-19 vaccine'. The Cyber Security Centre urged the Australian Government to:

> …continue to prioritise cyber security in the region, given more pronounced threat levels since the beginning of the pandemic, through the provision of technological and policy support and advice, along with other relevant measures.[67]

2.73 The School of Regulation & Global Governance at Australian National University advised that assistance in the Pacific region will have direct benefits in Australia, as the key to minimising harm in Australia 'will be assistance to less capable jurisdictions where shortages of material and expertise will be exposed by the pandemic's potential for rapid community spread'.[68]

2.74 The committee's COVID-19 crime inquiry reported that 'Witnesses advised that it is expected that this period will see intensified criminal activity driven from places such as the Pacific and Southeast Asia, compounded by increased demand, economic disruption, and rising unemployment'.[69] Much like vaccine related fraud experienced in Australia, these dire predictions have to date largely not manifested in the Pacific region.

2.75 Some of this avoidance of risk has been supported by Australian Government efforts, outlined below.

Responses to South Pacific threats

2.76 Australia has a long history of helping Pacific neighbouring nations, particularly in times of crisis. The Pacific Step-Up, first announced in September 2016, is one of Australia's highest foreign policy priorities. The programme further

---

65 Cyber Security Cooperative Research Centre, *Submission 3*, p. 6.

66 Cyber Security Cooperative Research Centre, *Submission 3*, p. 6.

67 Cyber Security Cooperative Research Centre, *Submission 3*, p. 7.

68 Australian National University, School of Regulation & Global Governance, *Submission 5*, p. 3.

69 Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, pp. 24–25.

enhanced Australia's commitments to assist in promoting the sovereignty, stability, security and prosperity of the Pacific region.[70]

2.77 The committee's COVID-19 crime inquiry report outlined:

> The committee acknowledges that Australia's law enforcement agencies already work closely with Pacific nations to address counterfeit vaccines and goods. However, the committee considers that law enforcement agencies could further assist Pacific nations to protect against counterfeit COVID-19 medical and pharmaceutical products through capacity building and training programs.[71]

2.78 The committee further noted in the COVID-19 crime inquiry report that this inquiry would be able to investigate this matter further. While this inquiry did not receive substantive evidence on Australian law enforcement agencies' role in protecting COVID-19 vaccine security and integrity, there is a wealth of publicly available information on what is being undertaken by those agencies. This information is outlined below.

2.79 The Pacific Step-Up programme has pivoted to address COVID-19 related challenges, with Prime Minister Scott Morrison stating, 'our Pacific island family must be a focus of international support. There has never been a more important time for Australia's Pacific Step-up as we all face these massive challenges.'[72]

2.80 Through this program, since January 2020, Australia has worked with Pacific island countries and Timor-Leste to help them prepare for and respond to the pandemic. Australia has provided the following:

- Responded to more than 120 requests from the region for assistance since January 2020.
- Adapted the aid program to provide immediate relief to help Pacific partners respond to the emerging health, economic, social and impacts of COVID−19.
- Provided COVID-19 testing kits, PPE, critical care equipment and other medical supplies to our region, including AUSMAT specialists to Papua New Guinea.
- Committed to procure and deliver COVID-19 vaccines to the Pacific, Timor-Leste and Southeast Asia, including $80 million to improve vaccine access for Pacific and Southeast Asian countries.

---

[70] Department of Foreign Affairs and Trade, *Stepping-up Australia's engagement with our Pacific family*, www.dfat.gov.au/geo/pacific/engagement/stepping-up-australias-pacific-engagement (accessed 23 July 2021).

[71] Parliamentary Joint Committee on Law Enforcement, *COVID-19, criminal activity and law enforcement*, p. 27.

[72] Prime Minister, the Hon Scott Morrison, MP, at extraordinary G20 Summit, 26 March 2020. See www.pm.gov.au/media/extraordinary-g20-leaders-summit (accessed 23 July 2021).

- Established a new, temporary $304.7 million COVID-19 Response Package over two years to help address the economic and social costs of the pandemic in the Pacific and Timor-Leste.
- Supported the delivery of new GeneXpert testing equipment, allowing Pacific island countries to detect and prevent the spread of COVID-19.[73]

2.81 Additionally, as Australia is an important transport hub for the region, the Australian Government has worked to maintain a transport corridor to the Pacific and Timor-Leste to allow for the movement of essential humanitarian and medical supplies from and through Australia. Through this transport corridor, Australia has delivered over 40 tonnes of humanitarian supplies to 13 Pacific island countries and Timor-Leste.[74]

2.82 The Australian Government also provided special screening measures at Australian airports to ensure that Pacific islanders and Timorese nationals around the world can transit through Australia to get home.[75]

2.83 The ABF is supporting regional developing and less developed countries by providing practical guidelines on the customs treatment of vaccines. These guidelines have been shared with Papua New Guinea and Border Five partners, and the World Customs Organisation has published the guidelines 'to support more effective enforcement activities against illicit vaccines and criminality in the supply chain globally'.[76]

2.84 Any assistance that Australia is giving to Pacific neighbours in relation to fraudulent vaccine certificates will be canvassed by the committee in the final report for this inquiry.

Committee view

2.85 It is clear that the pandemic brought with it a range of national-level concerns and challenges that went beyond the health and economic impacts of the disease. It is also clear that Australian law enforcement agencies were highly alert to those security and fraud issues, and took a very risk-conscious approach.

2.86 This risk-conscious approach has proved to be of significant benefit to the Australian community, as many of the predictions for fraud and security risks did not eventuate. From the evidence received by this inquiry, it does not appear that the potential crises were overstated. Instead, it appears the potential crises

---

[73] Department of Foreign Affairs and Trade, *Australia stepping-up to address COVID-19 in the Pacific*, www.dfat.gov.au/geo/pacific/australia-stepping-up-to-address-covid-19-in-the-pacific (accessed 23 July 2021).

[74] *Australia stepping-up to address COVID-19 in the Pacific.*

[75] *Australia stepping-up to address COVID-19 in the Pacific.*

[76] Department of Home Affairs, *Submission 4*, p. 3. Border Five is a forum on customs and border management issues, with participation from Australia, Canada, New Zealand, the United Kingdom and the United States.

were averted by early, strong and coordinated action from law enforcement agencies across Australia under various jurisdictions.

2.87 However, our nation is not out of the woods yet. The committee remains concerned that the issue of vaccine certificate fraud will arise in future, as governments look more and more to mass vaccination as the key defence against coronavirus. The committee has determined to publish its findings on other issues within this interim report, so that this inquiry can remain live to review the issue of vaccination certificates when they become relevant to the Australian context, noting this issue is arising in a rapidly changing environment.

2.88 There are also lessons that law enforcement agencies can take, and some improvements that can be made, including consideration of a permanent adoption of some temporary approaches taken during the pandemic.

2.89 The committee made several recommendations in the recent COVID-19 crime inquiry, and, as some of those recommendations are relevant to issues canvassed in this report, the committee affirms those recommendations below.

2.90 Firstly, the committee believes that the success of Australian law enforcement agencies to counter fraud and security threats during the pandemic relied heavily on the coordinated and joined-up approach taken. The committee believes it will be necessary to continue this approach, at least until the end of the pandemic.

2.91 The committee, therefore, affirms Recommendation 2 from its *COVID-19, criminal activity and law enforcement* inquiry report that:

> …the Australian Federal Police retain the Joint Intelligence Group, while any COVID-19 security risks remain, so they can continue to coordinate efforts across Australian law enforcement and intelligence agencies, and international partners.

2.92 Australian law enforcement and consumer rights agencies have long-standing approaches to both countering online fraud, as well as educating the public so individuals are better informed on how to protect themselves. While these efforts were stepped up during the pandemic, it is clear that a more sustained program of education is needed, not just in relation to COVID-19 related fraud.

2.93 The committee affirms Recommendation 4 from its *COVID-19, criminal activity and law enforcement* inquiry report that:

> …the Australian Government undertake public education campaigns on the prevalence and risks of scams and fraud.

2.94 While the evidence outlined in this report shows that assistance provided by the Australian Government to Pacific nations has had a positive impact, it will be necessary to continue this important work, particularly as international travel resumes.

2.95 The committee, therefore, affirms Recommendation 3 from its *COVID-19, criminal activity and law enforcement* inquiry report that:

> …the Australian Government ensures that assistance being provided to Pacific nations to counter the broad impacts of the pandemic, particularly the integrity and security threats to vaccines, continues until all such threats are no longer present.

Misinformation and disinformation

2.96 Misinformation and disinformation refers to 'manipulated narratives and campaigns' that are generally 'disseminated via the internet and social media channels'.[77] Misinformation refers to 'false information that was not created with the intention of hurting others', while disinformation is 'false information created with the intention of profiting from it or causing harm'.[78] This section will use the term mis/disinformation to cover both types of information.

2.97 The WHO, alongside other organisations such as the United Nations and the Red Cross, has declared that in addition to the COVID-19 pandemic, the world is experiencing an 'infodemic', defined as 'an overabundance of information, both online and offline…[including] deliberate attempts to disseminate wrong information to undermine the public health response and advance alternative agendas of groups or individuals'. WHO has stated:

> The Coronavirus disease (COVID-19) is the first pandemic in history in which technology and social media are being used on a massive scale to keep people safe, informed, productive and connected. At the same time, the technology we rely on to keep connected and informed is enabling and amplifying an infodemic that continues to undermine the global response and jeopardizes measures to control the pandemic.[79]

2.98 Digital advocacy group Reset Australia has monitored anti-vaxxer and conspiracy Facebook groups and found that membership has grown 280 per cent between January 2020 and March 2021 and argued that 'social media is contributing to vaccine hesitancy'.[80]

2.99 Deakin University submitted that, in some part due to misinformation, while vaccines are critical to the recovery of Australia, the way vaccines work and the

---

77 Cyber Security Cooperative Research Centre, *Submission 3*, p. 4.

78 World Health Organisation, *Let's flatten the infodemic curve*, www.who.int/news-room/spotlight/let-s-flatten-the-infodemic-curve (accessed 6 August 2021).

79 World Health Organisation, *Managing the COVID-19 infodemic*, 23 September 2020, www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (accessed 6 August 2021).

80 Shae McDonald, 'Members of anti-vaxxer and conspiracy theory Facebook pages skyrocket during COVID-19', *News.com.au*, www.news.com.au/technology/online/social/members-of-antivaxxer-and-conspiracy-theory-facebook-pages-skyrocket-during-covid19/news-story/8a966456ce3568080eb36761fa08cdd8 (accessed 23 July 2021).

minimal risks associated have not been clearly understood by the general public.[81]

2.100 The Cyber Security Centre submitted that researchers are concerned that 'despite their relatively small size and number of adherents, conspiracy theory narratives about the vaccine spread rapidly across the internet and could result in growing resistance to the vaccine and the undermining of efforts to establish herd immunity'.[82]

2.101 In early 2021, vaccine misinformation was targeting Australia's diverse communities via social media platforms, including Chinese platforms such as WeChat, with the Australian Broadcasting Corporation reporting it had the potential to significantly impact community trust in public health messaging.[83]

2.102 More recently, health professionals within migrant communities have said that misinformation spreading in culturally and linguistically diverse (CALD) communities has increased vaccine hesitancy, and have called on governments to counter this misinformation.[84]

2.103 Of particular concern is the spread of mis/disinformation in remote Indigenous communities, with the Indigenous Australians Minister, the Hon Mr Ken Wyatt MP, saying 'social media has been detrimental in some of the conspiracy theories' and has warned 'people spreading dangerous myths were putting Indigenous lives at risk'.[85]

2.104 Discouraging Aboriginal and Torres Strait Islander people from being vaccinated against COVID-19 is highly concerning, as not only do many live in remote communities with limited access to hospitals, but also underlying health conditions experienced in those communities create risky co-morbidities. Diabetes Australia has noted that 'people with diabetes are at higher risk of serious illness if they get COVID-19', which is concerning as 'Aboriginal and Torres Strait Islander people are almost four times more likely than non-Indigenous Australians to have diabetes'.[86]

---

81 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation, *Submission 6*, p. 6.

82 Cyber Security Cooperative Research Centre, *Submission 3*, p. 4.

83 Cyber Security Cooperative Research Centre, *Submission 3*, p. 4.

84 Tahlia Roy, 'Multicultural community leaders say COVID-19 vaccine misinformation failing to be dispelled by government programs', *ABC News*, 4 April 2021.

85 Daniel McCulloch, 'Conspiracies grip Indigenous communities', *Canberra Times*, 5 July 2021, www.canberratimes.com.au/story/7326099/conspiracies-grip-indigenous-communities/.

86 Diabetes Australia, *What you need to know about COVID-19*, www.diabetesaustralia.com.au/living-with-diabetes/covid19/ (accessed 6 August 2021) and *Aboriginal and Torres Strait Islander People*, www.diabetesaustralia.com.au/living-with-diabetes/aboriginal-and-torres-strait-islanders/ (accessed 6 August 2021).

2.105 Anti-vaxxer propaganda is also being spread widely in Asia, which may be of concern for Australia once international travel resumes, and unvaccinated people seek to enter Australia.[87]

Broader law and democracy impacts

2.106 The negative impact of mis/disinformation is not limited to the health responses against the pandemic, but also has an impact on law enforcement, democracy, and increases the risk of fraud.

2.107 The Cyber Security Centre argued that mis/disinformation relating to COVID-19 vaccines can in fact perpetuate telecommunications and internet fraud.[88]

2.108 WHO, the United Nations and Red Cross have declared that:

> …disinformation is polarizing public debate on topics related to COVID-19; amplifying hate speech; heightening the risk of conflict, violence and human rights violations; and threatening long-term prospects for advancing democracy, human rights and social cohesion.[89]

2.109 Home Affairs submitted that the Australian Government 'is increasingly concerned with COVID-19 disinformation affecting public discourse and democratic engagement' in a way that is not limited to incorrect health information, but is also 'manipulated information and propaganda, or political views from anonymous sources'.[90]

2.110 Dr Kaz Ross from the University of Tasmania, who researches Australian far-right extremists and conspiracy groups, has stated that far-right extremism 'has been on the rise in the past year in response to federal and state government handling of the coronavirus'.[91]

2.111 Throughout the pandemic, there have been protests against anti-viral measures such as facemasks, vaccinations and lockdowns. These protests divert hundreds of police officers to monitor the event, maintain public safety or make arrests for violent behaviour. Of significant concern, recent protests in Australia were organised, in part, by a German group that promotes 'anti-vaccine and COVID-19 conspiracy theories, as well as other conspiratorial content such as QAnon

---

87 Andreo Calonzo and Kwan Wei Kevin Tan, 'Anti-Vaxxer Propaganda Spreads in Asia, Endangering Millions', *Bloomberg*, 1 July 2021, www.bloomberg.com/news/articles/2021-06-30/anti-vaxxer-disinformation-spreads-in-asia-endangering-millions (accessed 6 August 2021).

88 Cyber Security Cooperative Research Centre, *Submission 3*, p. 4.

89 World Health Organisation, *Managing the COVID-19 infodemic,* 23 September 2020, (accessed 6 August 2021).

90 Department of Home Affairs, *Submission 4*, pp. 4–5.

91 Miki Perkins, 'Anti-lockdown protests a coalition of the alienated and the far-right', *Sydney Morning Herald*, 25 July 2021.

and Islamophobia'.[92] These links between Australian and German protest groups are a risk to Australia, because there has been a significant rise in far-right groups and protests linked to the pandemic in both Germany and France.[93]

2.112 There is also evidence that some Australian organisers of anti-lockdown protests are linked to other overseas far-right groups such as the Proud Boys, and are planning to introduce their COVID-19 related groups to more radical political views and encourage people to become more engaged in the political protest space.[94]

2.113 Additionally, there have been people who have individually protested against anti-viral measures by refusing to comply with check-ins or wearing facemasks in indoor public spaces. Police have been required to attend such instances, diverting them from other law enforcement work.

Responses to misinformation threats

2.114 The Commonwealth Fraud Prevention Centre is providing support to the Department of Health to 'assess and mitigate specific threats to the vaccination program' and is working to mitigate the risks of incorrect information through its 'Is it true' website.[95]

2.115 Home Affairs submitted:

> The Australian Government is increasingly concerned with COVID-19 disinformation affecting public discourse and democratic engagement – particularly the exploitation of social media to disseminate and quickly amplify manipulated information and propaganda, or political views from anonymous sources.[96]

2.116 Home Affairs advised that a range of agencies across the Australian Government 'are working to address disinformation in its various forms, whether that be anti-vaccination, foreign and electoral interference, COVID-19 or extremist disinformation'. Home Affairs submitted that it works with the Department of Health to promote factual information and to correct mis/disinformation about the vaccines and the rollout.[97]

---

92 Christopher Knaus and Michael McGowan, 'Who's behind Australia's anti-lockdown protests? The German conspiracy group driving marches', *The Guardian*, 27 July 2021.

93 'Anti-lockdown protests boost Germany's far-right, says security agency', *Reuters*, 15 June 2021 and 'France's far right take to the streets in protest of COVID-19 vaccine rules', *Associated Press*, 24 July 2021.

94 Michael McGowan, 'Where 'freedom' meets the far right: the hate messages infiltrating Australian anti-lockdown protests', *The Guardian*, 26 March 2021.

95 Attorney-General's Department, *Submission 10*, [p. 3].

96 Department of Home Affairs, *Submission 4*, p. 4.

97 Department of Home Affairs, *Submission 4*, pp. 4–5.

2.117 To ensure that culturally and linguistically diverse people can access appropriate information, Home Affairs has published a factsheet correcting the major misinformation claims about COVID-19 and COVID-19 vaccines, translated into 63 community languages. This factsheet is hosted online on Home Affairs' dedicated COVID-19 in-language website, and provided directly to communities through Home Affairs' community liaison officer network.[98]

2.118 The Cyber Security Centre recommended the Australian Government 'develop a greater awareness of current trends in misinformation and disinformation and to work hand-in-glove with social media companies to combat this growing threat'.[99] Home Affairs advised that it refers 'instances of mis/disinformation to digital platforms, for their consideration to remove for being inconsistent with their terms of service'.[100]

Committee view

2.119 It is clear that fraudulent COVID-19 mis/disinformation is leading to vaccine hesitancy, which is having the outcome of preventable serious illness and hospitalisations.

2.120 It has also become clear that COVID-19 mis/disinformation is not only leading to vaccine hesitancy, a health policy concern, but is also leading to some instances of civil disobedience and protest. COVID-19 mis/disinformation is therefore also a law enforcement issue of growing concern, particularly as individuals and groups become more radicalised.

2.121 Just as organised crime groups are manipulating people's natural fears during the pandemic to perpetrate fraud, other groups are also manipulating hesitancy with the new health measures of facemasks, mass vaccinations and lockdowns. This manipulation manifests itself first with previously law-abiding Australians engaging in acts of resisting health measures. However, in some instances, that resistance can grow into more concerning and ongoing behaviour.

2.122 All Australians, law enforcement agencies and governments must work together to ensure that when the pandemic is over, Australia is not left with the infectious disease of disinformation being used for fraudulent purposes, spreading fear and distrust of our necessary institutions.

2.123 It is of particular concern to the committee that mis/disinformation in Aboriginal and Torres Strait Islander communities and CALD communities could increase vaccine hesitancy, when many of these communities are already struggling with pre-existing health conditions, or distance from acute health care services. More must be done by all to ensure that these communities are supported to make

---

98 Department of Home Affairs, *Submission 4*, pp. 4–5.

99 Cyber Security Cooperative Research Centre, *Submission 3*, p. 4.

100 Department of Home Affairs, *Submission 4*, pp. 4–5.

informed health choices, which requires correct and up-to-date facts that are both based in health science as well as appropriate to their needs and circumstances.

Recommendation 1

2.124 The committee recommends the Department of Home Affairs ensure that the spread of COVID-19 misinformation and disinformation is monitored for extremist content and links to international extremist groups, as well as undertake greater efforts to counter misinformation and disinformation, especially among Aboriginal and Torres Strait Islander communities and culturally and linguistically diverse communities.

Mr Julian Simmonds MP
Chair

Appendix 1
Submissions

1 The Northern Territory Government
2 Australian Food Cold Chain Council
3 Cyber Security Cooperative Research Centre
4 Department of Home Affairs
5 ANU, School of Regulation & Global Governance
6 Deakin University: Centre for Supply Chain and Logistics and Centre for Cyber Security Research and Innovation
7 Medical Insurance Group Australia
8 Associate Professor Cassandra Cross
9 Australian Competition and Consumer Commission (ACCC)
10 Attorney General's Department
11 Pfizer Australia
12 *Confidential*
13 *Confidential*