Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Inquiry into vaccine related fraud and security risks

Parliamentary Joint Committee on Law Enforcement

30 April 2021

Introduction

The Department of Home Affairs welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement's (PJCLE) Inquiry into vaccine related fraud and security risks.

Vaccine rollout presents a range of criminal threats

International experience suggests criminal groups will try to exploit the vaccine rollout. In Australia's case, agencies advise this is likely to be on a small scale or isolated incidents. While some form of criminality associated with the vaccine rollout is expected, this is likely to be on a small or individual scale.

Potential threats the Government is monitoring include 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.

The Home Affairs portfolio contributes to whole-of-government efforts to facilitate legitimate COVID-19 vaccines across the border including securing the supply chain, while ensuring border controls remain effective in identifying and intercepting fake, counterfeit and diverted vaccines. Agencies are working together to identify vaccine related criminal activity, if and when it occurs.

Illicit vaccines and criminality in the supply chain

Illicit vaccines

A key threat to manage is the importation of illicit vaccines. Illicit vaccines include counterfeit, fake or unviable vaccines, and genuine vaccines diverted from overseas and domestic supply chains. Despite no illicit vaccines being detected at Australia's borders to date, and minimal detections worldwide, importations are being closely monitored. This active effort seeks to identify and disrupt any criminal actor seeking to exploit vulnerabilities in the vaccine program through illegitimate importation.

Should this threat eventuate, it will likely be small scale and demand driven by individuals who may attempt to import vaccines into Australia - either via online markets or through community connections. Attempted imports may increase as overall availability of vaccines increases globally.

Trends observed in Australia throughout the pandemic in relation to attempted importations of personal protective equipment, testing kits and substances purporting to treat COVID-19 indicate that there is a market for COVID-19 related products within Australia. The importation of illicit or low quality COVID-19 related items to Australia is expected to remain low.

The free vaccine rollout should minimise the demand from Australians seeking vaccines for their own supply. It is still possible some individuals or groups may seek to acquire specific brands or fast-track their own vaccination.

Criminality in the supply chain

It is 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.

The low demand and widespread distribution of a no-cost vaccine mitigates the organised crime threat in Australia. The impact of organised criminal activity associated with COVID-19 vaccines in Australia is likely to be limited to scam attempts and small scale black market activity. Onshore criminals may also resort to illegally refilling empty vials. Procedures for the correct disposal of vials mitigate this risk.

Current responses

Home Affairs agencies are, through the work of a joint operation, contributing to whole-of-Government efforts to facilitate legitimate COVID-19 vaccines across the border, while ensuring border controls remain effective in identifying and intercepting fake, counterfeit and diverted vaccines as well as other illegitimate medicines.

The ABF continues to contribute to the logistics network design for the movement of vaccine products facilitated and implemented by the Department of Health. By doing so, 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.

The ABF in partnership with the Department of Home Affairs is proactively assessing the threat posed by trusted insiders across the vaccine supply chain and will continue to work across Government to ensure adequate risk controls are in place for the secure transport of legitimate vaccine products.

The ABF continues to inform its approach through regular engagement with key industry bodies and international partners, contemporary intelligence, law enforcement and whole-of-government partners, and the experience of key stakeholders. This helps identify supply chain vulnerabilities and implement effective, innovative and multidisciplinary responses leveraging the full operational, regulatory and enforcement capabilities of the ABF to assure Australia's supply chain integrity.

ABF officers have received specialised training by vaccine manufacturers to assist in real time identification of potential illegitimate vaccines. In addition, the ABF, AFP and Therapeutic Goods Administration are working closely to share relevant information and intelligence in relation to counterfeit and unapproved therapeutic goods.

Additionally, the ABF will participate in World Customs Organisation Operation STOP II, which commenced 1 April 2021 and involves the intelligence led targeting of cargo suspected of containing COVID-19 related illicit goods. Counterfeit vaccines are a particular focus of this operation, which will involve up to 183 partner agencies across the globe, real time sharing of information and intelligence fusion. It is expected to enhance the ABF's understanding of the global threat picture.

Drawing on its operational experience with vaccine facilitation and enforcement, the ABF has developed practical guidelines on the customs treatment of vaccines to support developing and less developed countries. The ABF has shared the guidelines with the Papua New Guinea Customs Service and Border Five partners to assist their customs handling of vaccine consignments. The World Customs Organisation has also published the guidelines and shared them with national customs administrations, to support more effective enforcement activities against illicit vaccines and criminality in the supply chain globally.

The Department of Home Affairs has established a joint intelligence construct with portfolio and partner agencies to support the whole-of-government effort on the COVID-19 vaccine rollout. This intelligence-led effort involves a dedicated analytic focus and an inter-agency group to inform on specific threats including: the facilitation and legitimate trade of approved COVID-19 vaccine imports; and illegitimate trade of COVID-19 vaccines. This joint taskforce leverages the collective intelligence assessment of the National Intelligence Community and international stakeholders.

The AFP has created Taskforce LOTUS to respond to persons and organised crime entities who plan to commit criminal acts related to the rollout of the COVID-19 vaccine in Australia. This was established on 8 February 2021, in advance of the vaccine rollout to support a quick operational response.

Through LOTUS, the AFP will assist Commonwealth partners in investigating COVID-19 vaccine crimes that are multi-faceted and span serious and organised crime involvement in crimes ranging from the mass theft of vaccines through to fraud-related scams against Commonwealth procurements and grants.

The Transport Security Amendment (Serious Crime) Bill 2020 (the Serious Crime Bill) is currently before the Senate. The Serious Crime Bill will assist in combatting serious criminal influence at security controlled airports and seaports by introducing an expanded eligibility criteria for applicants and holders of aviation and maritime security identification cards (ASICs and MSICs). A key supply chain vulnerability is corruption of trusted personnel at various points of the supply chain. Passage of the Serious Crime Bill will help reduce the ability of serious and organised crime groups to use and recruit trusted insiders who have access to the most secure and vulnerable areas of airports and seaports. The Serious Crime Bill will ensure that only the most trusted individuals have unescorted access to secure areas at airports and seaports and addresses this vulnerability in the vaccine supply chain.

Government collaboration with pharmaceutical companies has also enhanced the security of the supply chain which is highly likely to deter criminal actors by limiting opportunities for compromise.

Cybercrime and fraud

Criminals have taken advantage of COVID-19, using community concerns about the pandemic as a theme for fraud and scam activity. It is likely that fraud and scam activity driven by the release of the COVID-19 vaccine will be the most significant criminal issue associated with COVID-19 to impact Australia over the next 24 months.

Criminals will likely use vaccine-themed phishing campaigns and other scams to obtain Personal Identification Information (PII), which they may then exploit for future fraud. It is likely cybercriminals will first target the specific sectors identified as priority vaccine recipients. Of particular concern are the elderly due to their heightened vulnerability to scam activity.

Cybercriminals may seek to acquire sensitive Medicare and MyGov PII via fake online COVID-19 vaccination sales. Additionally, phishing activity impersonating health services and the Australian Government may procure sensitive PII by way of online registration.

Sensitive PII accessed via scam COVID-19 vaccination sales or registration may be on-sold to cybercriminals or exploited for future fraudulent activity, including but not limited to: banking and credit card fraud, superannuation fraud, tax fraud, Medicare fraud, and Centrelink fraud.

Deliberate ransomware infections pose a high threat to organisations involved in Australia's COVID-19 vaccine supply chain. Broader ransomware targeting of Australia's health care, manufacturing and logistics organisations, amongst others, may disrupt the COVID-19 vaccine supply chain.

Current responses

The Department of Home Affairs 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. The Department of Home Affairs has also established a new working group with the National Australia Bank to explore opportunities for collaboration to address these crimes.

As part of Australia's Cyber Security Strategy 2020, Home Affairs has also 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.

Home Affairs' national identity-matching services, including the Document Verification Service and Face Matching Services, are key to combatting identity fraud. The services provide a fast, secure, online check of identity information against government identity records.

The Face Matching Services will make driver licence images matchable for the first time, subject to the passage of the Identity-matching Services Bill 2019 currently before Parliament. This initiative improves 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. The identity-matching services will also underpin Australia's transition to a digital economy by providing a secure online service to verify that the biographic and biometric details relied on to create digital identities match against original government records.

Cyber security incidents may increase throughout the COVID-19 vaccine's research, manufacture, distribution and administration phases, and organisations should maintain a heightened state of cyber threat awareness.

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. A range of portfolios 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. Throughout the pandemic, Home Affairs has contributed to limiting the spread of potentially harmful COVID-19 and COVID-19 vaccine mis/disinformation online, by referring instances of mis/disinformation to digital platforms, for their consideration to remove for being inconsistent with their terms of service.

Home Affairs continues to work with the Department of Health to publish and distribute factual information about the rollout of the COVID-19 vaccines and to correct mis/disinformation about the vaccines and the rollout. Home Affairs has published, with the Department of Health, a factsheet correcting the major misinformation claims about COVID-19 and COVID-19 vaccines. The factsheet is translated into 63 community languages, hosted online on Home Affairs' dedicated *COVID19inlangague* website, and provided directly to communities through Home Affairs' community liaison officer network.

At the Commonwealth officials level, the Criminal Justice Law Enforcement Forum (CJLEF) is driving an integrated response to COVID-19 criminality. CJLEF is an agency head level forum consisting of 17 Commonwealth agencies.

Since COVID-19 began, CJLEF has explored the impact of COVID-19 on organised crime groups and opportunistic criminals and the evolving threat picture. This has increased visibility across agencies of various lines of effort, particularly to better coordinate public messaging for greater public confidence in the vaccine program, and reduce opportunities for scam and fraud activity.