CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Inquiry into COVID-vaccine related fraud and security risks

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Inquiry into COVID-vaccine related fraud and security risks

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into COVID-vaccine related fraud and security risks. We commend the Federal Government for its ongoing commitment to ensuring Australia remains a safe and secure nation and a leader in COVID-19 vaccine rollouts.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre

Executive Summary

COVID-19 has indelibly transformed the world in which we live. More than a year into the pandemic, the world has undergone a period of intense fluctuation – economies have stalled, borders have closed, and long-established global supply chains have been markedly disrupted. Perhaps most significantly, COVID-19 has dramatically impacted the way we live and work. Globally, the online dependency of workers has grown exponentially since the beginning of the pandemic. And in the mass migration to working-from-home (WFH) conditions, many workers and organisations have found themselves with less-than-optimal cyber security protections and inadequate cyber awareness.

Concurrently, cyber criminals have upped the ante. COVID-19 has been leveraged by nefarious cyber actors to market fake vaccines and vaccine certifications; launch sophisticated attacks on vaccine manufacturing facilities and hospitals; and spread vaccine misinformation and fear amongst populations. Individually and collectively, citizens around the world are now facing a greater volume and range of cyber threats. And as the pandemic continues, there are no signs these threats will abate. During the COVID-19 lockdown period, Australia witnessed an exponential rise in cyber activity by malicious cyber actors, with the Australian Cyber Security Centre (ACSC) noting in 2020 they had fielded almost 60,000 reports from Australian individuals and organisations purporting instances of cybercrime.

Early in the pandemic, the health sector also found itself in the crosshairs. In a May 2020 joint statement, the Department of Foreign Affairs and Trade (DFAT) and the ACSC warned that malicious cyber activity was targeting "the operation of hospitals, medical services and facilities, and crisis response organisations outside of Australia". As nation states now pivot to the delivery of nationalised mass vaccine rollouts, a subsequent rise in COVID-19 vaccine related cyber threats is being experienced globally, indicative of the ability of cyber criminals to adapt to amorphous environments. These are likely to escalate, morph and mutate as the pandemic continues and the world becomes ever more digitally interconnected. Similar to what is taking place elsewhere, Scamwatch has warned the public of scams related to COVID-19 vaccinations in Australia, many of which are disseminated via online means. Even supranational governance institutions are not immune. The World Health Organization (WHO) issued a public alert noting that hackers and cyber scammers have been impersonating the organisation by sending emails and WhatsApp messages containing malicious links.

It is timely, therefore, to evaluate how Australia can most effectively respond to and prevent any current or future COVID-vaccine related fraud and security issues. The CSCRC notes this inquiry will be beneficial for Australia's own vaccine program, which will ensure the future health, security and prosperity of our nation.

Telecommunications and internet fraud relating to COVID vaccinations:

As COVID-19 lockdown restrictions around the globe have eased and as governments proceed with mass vaccination plans, there has been a sharp surge in telecommunications and internet fraud relating to COVID-19 vaccinations. This activity has come alongside and indeed, been *perpetuated by*, a proliferation of misinformation and disinformation pertaining to COVID-19 vaccines, sown by various actors for political and economic gain.

2020 was the year the words 'disinformation' and 'misinformation' came to the fore – manipulated narratives and campaigns undertaken by the aforementioned range of actors. Frequently disseminated via the internet and social medica channels, the widespread impacts of this phenomena over the past year are due, in no small part, to their pronounced focus on the COVID-19 vaccine. Diverse COVID vaccine-related conspiracy theories have flourished and demonstrated significant impact and reach. A May 2020 American survey found that almost half of Republicans and approximately 20 per cent of Democrats believed billionaire Bill Gates to be at the helm of a global plot to implant people with microchips. Accordingly, researchers studying anti-vaccination movements have warned 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.

Such concerns have been echoed in Australia. In March 2021, the ABC (Australian Broadcasting Corporation) reported vaccine misinformation was targeting Australia's diverse communities via social media platforms. Most notably, this activity was evident on Chinese social media platforms such as WeChat, with the ABC reporting it had the potential to significantly impact community trust in public health messaging. One of these social media posts falsely claimed that mRNA vaccines, such as Pfizer's, could genetically modify humans, and was shared with more than 2000 members. There is urgent need for the Australian Government and relevant policymakers to 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.

The concurrent rise in cyber-related COVID vaccine fraud is a worldwide phenomenon. In the UK and since the beginning of the pandemic, more than 6000 cases of COVID-related fraud and cyber-crime have been reported by the UK's Action Fraud team. This spike in activity comes alongside a pronounced uptick in cyber attacks against the UK's pandemic response infrastructure, with the National Cyber Security Centre (NCSC) reporting it is responding to approximately 30 "significant attacks" per month, notably targeting vaccine producers and vaccine supply chains. This echoes what has been reported in the United States. As fraudsters seek to capitalise on widespread confusion and uncertainty about the vaccine, relevant government bodies have warned American citizens to be on guard concerning COVID vaccine scams, which have included:

- the sale of medically unproven products such as teas or 'immune shots' claiming to prevent or treat COVID-19 and/or deliver the same benefits as a vaccine;
- websites and online bazaars claiming to offer legitimate vaccines for sale;
- the deployment of social media posts, emails, text messages and robocalls to offer Americans seemingly legitimate opportunities to leapfrog vaccination queues via fake vaccine registration websites;
- people posing as medical experts and administrators of purported COVID-19 vaccines, which are 'sold' to citizens.

In response, the United States' Federal Drug Administration (FDA) has established a Fraudulent Products Task Force to quell such fraudulent activity. It works in collaboration with relevant government partners to prevent illicit and potentially unsafe vaccines from circulation to the public. Furthermore, the FDA has enhanced efforts to keep the public informed of COVID-19 vaccine fraud.

In Australia similar fraudulent trends have been observed. Cyber criminals are preying on citizens' anxieties and uncertainties, along with less secure WFH conditions to take advantage of the COVID-19 vaccine rollout through online scams. The Australian Communications and Media Authority (ACMA) has advised 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. The ACSC has also been actively advising Australians of current COVID-19 related vaccine scams, along with providing some relevant tips about how to discern their lack of legitimacy. And the Australian Competition and Consumer Commission's (ACCC) Scamwatch has built a COVID-19 scam portal highlighting all current coronavirus-related scams, noting that since the beginning of the pandemic, there have been more than $9,800,000 AUD in reported losses. The website provides a list of the most prevalent vaccine-related online scams, including:

- 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.

The ongoing public messaging concerning these cyber-perpetuated scams and schemes is commendable. However, 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.

Criminal activity around the supply of fake vaccines, black market vaccines and/or fake vaccine certifications and the acquisition of certificates:

Alongside the emergence of COVID-19 fraud relating to vaccines, criminal activity around the supply of fake vaccines, black market vaccines and/or fake vaccine certifications and the acquisition of certifications has materialised. This has occurred against the backdrop of the quick development of vaccines, insecure supply chains and an unequal distribution of vaccines across socioeconomic demographics of society and between wealthier and less developed countries. On 16 April 2021, the Director-General of the World Health Organization (WHO) warned the United Nations Economic and Social Council global vaccination efforts are, at present, marked by stark inequality: 82 per cent of vaccines already deployed have been distributed to high or upper-middle-income countries. This equates to 25 per cent of people in high-income countries as opposed to one in 500 persons in low-income countries.

Furthermore, such inequality introduces the very real risk of corruption in the manufacture, allocation and distribution of vaccines. This is a contributing factor to the growing black market for fake vaccines. A recent United Nations Office on Drugs and Crime (UNODC) report underscored the sobering risks which come alongside corruption, that may threaten public health goals and continue to prop up a vaccine black market, including the "entry of substandard and falsified vaccines into markets, theft of vaccines within the distribution systems, leakages in emergency funding designated for the development and distribution of vaccines, nepotism, favouritism, and corrupted procurement systems" (p 1). The report warns of the particular dangers of substandard and falsified vaccines and COVID-19 medical products entering the global market, trafficked by organised crime groups who are capitalising on corruption, limited vaccination supplies and lucrative potential profit margins (p 6).

In March 2021, Interpol issued an advisory that counterfeit vaccines were circulating, after taking down a fake COVID vaccine distribution network across two continents. And in recent weeks Australia has seen one of the world's leading manufacturers of the COVID-19 vaccine, AstraZeneca, advise Australians to be wary of third-party suppliers offering the vaccine directly, amid concerns they might be counterfeit. In light of these threats, it is vital to amplify public messaging advising all Australians that vaccines are not available for private sale. Legitimate vaccines can only be administered through registered health providers who have received the vaccine directly via government, not through any other means.

It should also be highlighted that much of this illicit activity is taking place online and increasingly on the dark web. In the United Kingdom, the sale of COVID-19 vaccine passports on the darknet have been identified, going for as little as $150 USD. Despite the low price tag, a recent report underscored the opportunity for cyber criminals to capitalise on huge opportunities for profit – with prices for COVID-19 vaccines varying from a few hundred dollars to upwards of a few thousand. Unfortunately, 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.

Hence, there is an urgent need for relevant Australian law enforcement agencies, including the Australian Federal Police, to be equipped with the appropriate resources and legislated powers to ensure the transparency, security and legitimacy of Australia's COVID-19 vaccine program. While the Therapeutic Goods Administration (TGA) is already working in collaboration with government to prevent the illicit trade of vaccines, government and relevant law enforcement agencies and organisations also have a pivotal role to play. This could include enhancing existing security measures for vaccine programs to deter counterfeit efforts, such as the development of security systems that will work to prevent forgeries and more effectively track emerging and current threats to vaccine security. These efforts will not only increase the effectiveness of Australia's vaccine rollout but provide Australian citizens with confidence and assurance in the safety of our nations' vaccine program.

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:

The CSCRC notes the longstanding partnership between Australia and the South Pacific nations, and the integral spirit of cooperation, collaboration and respect that defines these relationships. Australia has long been a committed partner of the South Pacific, working to build a strategically secure region and ensure its economic and political sovereignty. It is also a cornerstone of Australian foreign policy, with the 2016 announcement of the Pacific 'step up', later supported by the 2017 Foreign Policy White Paper, which outlined Australia's agenda for ensuring security and prosperity in the region. Key to the bolstered support entailed under the Pacific 'step up' is:

- a renewed focus on mitigating security challenges
- an expanded Cyber Cooperation Program to:
    - strengthen cybercrime prevention, prosecution and cooperation
    - enhance cyber incident response capability, and
    - foster best practice use of technology to support economic growth and sustainable development.

Noting these security priorities, Australia has a significant role to play in assisting regional partners both during and after the pandemic. This assistance pertains to both cyber security challenges and support concerning any issues of fraud and integrity risks related to the COVID-19 vaccine. There is urgent need for Australia to work closely together with our Pacific partners to mitigate cyber security risks, with a January 2020 Standards Australia report, the *Pacific Island Cyber Security Standards Agenda*, noting that Australia remains one of the most highly targeted 'test beds' for ransomware and spear-phishing attacks. The report presents recommendations as to how the region can best align to international cybersecurity standards and ultimately uplift its cyber security posture. The CSCRC urges 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.

The CSCRC notes the sobering economic impacts the COVID-19 pandemic has had on the Pacific region, which is heavily reliant on tourism. The Center for Strategic and International Studies (CSIS) has noted the dire consequences this has had on populations in the region. It estimated the number of residents in the region living in extreme poverty could increase by 40 per cent. To help maintain political stability in the region and protect against risks of corruption and disingenuous foreign influence, economic assistance from developed countries, Australia included, is required. This could be provided via emergency financing and the suspension of debt.

Australian-led assistance in the region remains all the more relevant given the challenges currently being experienced across the Pacific Island nations' vaccine distribution programs. Despite the establishment of the Pacific Humanitarian Pathway on COVID-19 by Pacific Island nations in April 2020 to facilitate regional COVID-19 relief efforts, by and large, programs were expedited and developed in ad-hoc fashion with little regional cooperation. Throughout the pandemic, the agreement promised the "expediting of medical assistance, expediting customs clearance of medical supplies, and facilitating diplomatic clearances for chartered flights and commercial shipping" but these measures have not been fully realised. In addition to the failure of the Pathway to provide working frameworks for effective regional collaboration, existing security and cooperative regional forums remain fractured, with nations un-unified. This threatens to hamper the effective, safe and secure delivery of vaccines across the region. On the latter point, Papua New Guinea, Fiji and the Solomon Islands are not expected to achieve mass vaccination until 2025, which will impinge borders reopening and the reset of tourism economies to pre-pandemic levels. Such problems are more concerning, given rising geopolitical tensions and increased strategic competition in the Indo-Pacific. China has demonstrated ongoing efforts to bolster its military, diplomatic and economic presence in the Pacific Islands, with plans announced to provide coronavirus vaccines in the region. This attempt to wield soft power through 'vaccine diplomacy' comes alongside significant Chinese capacity building efforts in the region. To this end, it is essential the Federal Government continues its efforts to support the region through the safe provision of effective vaccines to Pacific Island populations and through ongoing capacity building initiatives.

Accordingly, the CSCRC welcomes the Federal Government's March 2021 commitment to boost vaccine coverage in the Pacific region, with the distribution of up to one million COVID-19 vaccine dosages. This comes several months after a November 2020 Australian government pledge for the provision of an additional $500M AUD over three years (on top of an already committed $23.2M AUD) to support the rollout of vaccines in the Pacific region and Southeast Asia. Significantly, these funds will be utilised to effectively distribute the vaccine across the region and work to ensure the safety, efficacy and quality of the vaccine according to global best practice public health advice.

Furthermore, they will assist in the return to 'normalcy' for the region, stimulating economic growth and working to ensure a thriving, shared economic future for the region. These funds come alongside a March 2021 pledge from the Quad to boost the delivery of the Johnson & Johnson vaccine across the Indo-Pacific.

Physical security in the production, transport and supply of COVID vaccines in Australia:
&
Measures to prevent and protect against COVID vaccine-related fraud and security risks

The CSCRC notes the integral role that supply chains and logistics play in the production, transport and supply of COVID vaccines in Australia. Central to this is the cyber security and cyber resiliency of these supply chains, which ensure the integrity of vaccine supplies from inception through to global distribution. In a world of increasing digital interdependency, notably the reliance on global technology solutions produced by large multinationals, it remains an imperative to ensure the security of software systems and relevant data. The recent SolarWinds cyber espionage operation, the "largest and most sophisticated attack the world has ever seen", demonstrated the efficacy of cyber hackers and tools and techniques to impact multiple and seemingly unrelated software systems. Ensuring the security of these supply chains will, by extension, work to ensure the integrity of vaccines, the supply chain and the physical security of COVID vaccines.

Cyber attacks remain a real and present threat to physical storage locations of vaccines at medical facilities globally, recently touted as the "most valuable cyber target in the world". In July 2020, it was disclosed that state-based cyber actors from Russia and North Korea had targeted vaccine production facilities with cyber attacks. This was followed by an October 2020 hack on Dr Reddy's Laboratories, the Hyderabad-based laboratory approved to manufacture Russia's Sputnik V vaccine. The data breach forced the shutdown of its manufacturing facilities, demonstrating the tangible impacts that cyber attacks can have on the supply of COVID vaccines. In Australia, although no vaccine facility has been targeted, the March 16 ransomware attack on a Melbourne health organisation and the April 26 cyber attack on UnitingCare in Queensland, which runs dozens of hospitals and aged care homes, are sobering reminders that healthcare facilities and the systems they run remain vulnerable to cyber hacks. The latter attack knocked the organisation's systems offline, impacting the ability of doctors to provide essential services to patients. Furthermore, considering the Pfizer vaccine needs to be kept at normal freezer temperatures for up to two weeks during transport (and at regular fridge temperatures for up to five days), ensuring transport and logistics companies are cyber secure and resilient will ultimately assist in Australian vaccination administration efforts.

Proposed legislative and regulatory changes under the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill), will assist in bolstering the cyber posture of Australia's critical infrastructure. The Bill aims to capture 11 critical infrastructure sectors (as opposed to the previous four), including the health care and medical sector and transport. Further, there is also more work to be done in Australia to ensure that in the case of a cyber attack on medical and research facilities, that public accountability is front and centre. That is, ongoing transparency and support from government will assuage fears from organisations about publicly disclosing details about data breaches and/or cyber attacks, ultimately contributing to greater information and intelligence sharing and cyber uplift.

As a liberal democracy, Australia has a proud tradition of charting an effective course between maintaining the rule of law and adhering to democratic checks and balances. Accordingly, the CSCRC urges the Federal Government to maintain its strong stance in the international community on promoting cyber norms and behaviours. Central to this is alignment with our Five Eyes and Quad allies in 'calling out' illegal or unacceptable cyber behaviours.

Finally, more work can be done to educate all Australians about COVID vaccine-related fraud and security risks. Although the Australian Government and relevant organisations have proven to be effective and coordinated in disseminating public messaging about COVID-19 related fraud and cyber security risks, there is a growing risk of *public complacency.* This is especially relevant given Australia's success at containing the spread of the virus. However, a corollary effect is the 'tuning out' of citizens' to messaging campaigns, including those on cyber security threats. Given the increasing sophistication in the variety of cyber attacks during the pandemic, there is a need to distil efforts to target the public with effective messaging campaigns about how citizens and organisations can protect themselves, their digital assets and their data. Campaigns and resources such as those run by the ACCC's Scamwatch remain highly effective, and ongoing updates to ensure these resources remain relevant and offer timely advice is crucial.

In relation to this, considering the high levels of misinformation and disinformation proliferating across social media accounts about COVID-19 vaccines and gaining access to them, the CSCRC urges the Federal Government to double-down on efforts to counter these unhelpful narratives, by providing clear and concise advice.

Despite Australia's fortunate position in the world as it comes to post-COVID-19 recovery, if present levels of coronavirus cases globally persist, it is likely that COVID-19 vaccine fraud will remain a threat. Given the transnational nature of cyberspace and the law enforcement challenges this presents, many cyber criminals are able to operate without impunity. Accordingly, efforts to prevent against future attacks must be built around a strong supply chain, ongoing public awareness campaigns and cyber hygiene education to achieve long-lasting and effective societal cyber uplift.