Department of Foreign Affairs and Trade

RG Casey Building, John McEwen Crescent,

Barton ACT 0221 Australia

16 June 2020

RE: Call for Submissions: Cyber and Critical Technology International Engagement Strategy (CCTIES)

My name is Dr Cassandra Cross and I hold a position as a Senior Lecturer in the School of Justice, Faculty of Law, at Queensland University of Technology. My area of expertise targets (online) fraud, but also encompasses related areas such as identity crime, data breaches, cybercrime, and cybersecurity more broadly. I first started researching fraud in 2008, while working as a civilian with the Queensland Police Service. In 2011, I was awarded a Churchill Fellowship to explore the prevention and support of online fraud victims. This enabled me to travel across the UK, US, and Canada to engage with over 30 agencies working in this space. It was an invaluable experience which was the catalyst to my academic transition.

My appointment to QUT in September 2012 has enabled me to pursue a research agenda focused solely on fraud. I have developed an extensive and authoritative track record in this area, across both national and international fronts. I have published over 50 outputs predominantly relating to fraud and cybercrime. I have been successful in bidding for, and attracting research funding, having led eight research projects, all in collaboration with government or industry partners.

In exploring fraud, my research has focused heavily on victim perspectives of these crimes. I have spoken directly with over 150 victims of fraud and other cybercrimes, who have shared with me the financial, physical, and social impacts of these incidents. Too often, they have described the trauma and harm they have experienced at the hands of offenders, but also at the hands of the system. Fraud victims (and cybercrime victims more broadly) overwhelmingly speak of the negativity of their experiences in navigating the criminal justice system to seek an appropriate response to their victimisation. Sadly, this is not relegated to Australia, but is mirrored across other countries such as the UK, US, and Canada.

The following submission draws on my decade of research and experience in this area to advocate for these victims to be included in the future policy direction of this area. Too often, the "human" element of cybercrime and cybersecurity is forgotten, with a strong focus on the technology which enables and facilitates incidents to occur. This has been to the detriment of many individuals, who have neither felt acknowledged in their victimisation, nor supported in their recovery. My intention for this submission is to give a voice to those who find themselves on the wrong end of cybercrime and cybersecurity and are powerless to advocate for change in their own situation. Collectively, there is much to be done to improve the current response to those who experience negative outcomes of engaging with technology, across both cybercrime and cybersecurity contexts.

I thank DFAT for the opportunity to contribute to the development of the revised strategy.

Dr Cassandra Cross
School of Justice, Faculty of Law, Queensland University of Technology

E: ca.cross@qut.edu.au P: 07 3138 7131

The following submission puts forward observations and findings from my collective research into fraud (and related cybercrime) victimisation. It draws on my knowledge and communications with scholars, law enforcement and industry bodies spanning Australia and overseas. Further, it draws predominantly from the Cybersecurity and Cybercrime sections of the previous *Australia's International Cyber Engagement Strategy* (2017).

What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?

The evolution of technology provides immeasurable benefits to consumers both Australia and worldwide. It is particularly difficult to think how society would have coped with the recent lock down and isolation restrictions imposed by government to combat COVID-19 without the use of technology. However, with this comes immense challenges and a range of risks which threaten the livelihoods of individuals and businesses alike.

The previous *Australia's International Cyber Engagement Strategy* (subsequently referred to as AICES) had a strong emphasis on education and prevention with regards to cybersecurity and cybercrime. Further, there was a clear focus on the willingness and desire to collaborate with other relevant parties to enhance and improve work in these areas. This proactive approach to both areas of cybersecurity and cybercrime is to be applauded. It is much better to prevent an incident or crime from occurring in the first place, rather than seeking to rectify it once it has occurred. This is a positive way of approaching this area which should continue into the next version.

However, it is inevitable that prevention and education will not always be successful. Sadly, despite the best efforts of all involved, there will be individuals and organisations who are victims of cybersecurity incidents or cybercrimes. The requirement to respond to victimisation is currently missing in the AICES and in much of the broader discussion that relates to these areas. Not only should the strategy seek to provide goals for the prevention of these occurrences, but it should also acknowledge the reality that incidents will occur. As a result, the strategy should seek to advocate a response that is appropriate to the situation and those involved. Further, it should mandate the provision of support to assist in the recovery of victims and the building of resilience to protect against future and/or ongoing victimisation.

In talking to those who have experienced fraud (and related cybercrimes) across many years, they detail many horrific stories of victimisation. However, in addition to what they experience at the hand of their offender/s, they further describe the additional trauma and suffering they have received at the hands of the those they seek a response from. Fraud is arguably different from many other offence types, in that there are a range of agencies who can potentially respond to victimisation. This includes traditional law enforcement (at different levels) but also extends to consumer protection, banks and financial institutions, remittance agencies, other government, and non-government bodies as well as industry (depending on the circumstances of their incident). This array of agencies has been termed the "fraud justice network" and victims experience significant barriers in seeking a response. Often, victims are unable to lodge a complaint with any one agency and are instead referred to other agencies, in what is termed the "merry-go-round" effect. This is not isolated to an Australian context but is consistently experienced by victims in other countries. The introduction of the ReportCyber portal and the former Australian Cybercrime Online Reporting Network (ACORN) attempt to overcome this but have not been successful from a victim perspective.

Further, there is a strong stigma associated with fraud victimisation. In many circumstances victims have actively participated in the sending of money or personal information (albeit under deceptive

pretences) and are subsequently blamed for what has happened. Victims have detailed countless scenarios where they were openly held responsible for their actions by police and other agencies and were often humiliated in seeking help for what had occurred. The shame and embarrassment associated with fraud (and other types of cybercrime) victimisation is a barrier that prevents many from disclosing and seeking help in the first place and further deters those who attempt regardless. In this way, offenders use the shame and embarrassment to isolate the victim and this contributes to the ongoing success of offenders.

Currently, society lacks the recognition they could be vulnerable to fraud or cybercrime. Nobody thinks that it will happen to them; there is a strong belief that one is too smart or too savvy to ever be a victim. This fails to acknowledge the skill of the offender, who can easily identify the weakness of a potential victim and exploit it. It also prevents society from having constructive conversations around victimisation, a conversation that is void of judgement and instead promotes collective learning and awareness of individual vulnerabilities, and of how to respond practically to victimisation.

Victims overwhelmingly wish to be acknowledged. They desire the ability to tell their story, to be listened to and to not be judged for what has occurred. In many cases, this acknowledgement and procedural request is above their need and desire for an individual outcome for their case. It would also work towards a notable improvement on levels of satisfaction related to their interactions across the fraud justice network. Levels of satisfaction with fraud victims in their interactions with agencies across the fraud justice network are consistently low both here in Australia as well as overseas.

A revised AICES has the potential to propel this much needed societal change. By recognising the inevitability of victimisation, a revised strategy has the potential to normalise constructive conversations in the area. It further gives a legitimacy to victims in their interactions with relevant organisations and should provide a minimum level of response, one that seeks to empower victims in addressing their situations rather than exacerbating any suffering they have already incurred.

Further, a revised AICES can drive an agenda for change around supporting those who have experienced victimisation across cybersecurity and cybercrime contexts. While continuing to focus on the proactive needs in this space, there is also a corresponding requirement to focus on the reactive needs of these individuals and groups. Currently, this is largely ignored to the detriment of those who experience victimisation.

How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

Offending takes place within a global context. This poses many genuine challenges to police and other agencies who seek to respond to fraud and related cybercrime victimisation. Policing is still heavily founded upon geographical boundaries, which restrict their power and authority to investigate incidents which usually span multiple jurisdictions. This is not only problematic within Australia between state and territory borders but is clearly an issue for those in Australia who are targeted from international destinations. Correspondingly, legislation is also largely tied to geographical boundaries, which poses difficulties in being able to prosecute offences.

There is a pressing need to better navigate the challenges posed by current approaches to sovereignty and jurisdictions. While there are several agreements in place at different levels to theoretically overcome this, in reality they are cumbersome and present as a barrier to progress for many victims.

With the increased connectivity of Australians worldwide, it is no longer appropriate to tell victims that simply because their offender is potentially located overseas, that there is nothing that can be done. Offenders act with impunity across most of their offending in cybercrime, using jurisdiction (amongst other factors) to their advantage.

The current AICES places a strong emphasis on the need to build international relationships across the globe to tackle these issues. This arguably remains an important focus and must be continued. However, there is an additional need to drive practical changes at a grassroots level (local police and other relevant agencies) across both national and global contexts. This needs to overcome some of the administrative and bureaucratic challenges that these issues currently pose and can provide real change for victims.

What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?

In terms of fraud, the flow of money is a vital part of offending. The increased ease of transferring money across local and international contexts has substantial implications for offending. In my own research I have seen an evolution in payment types and requests for fraud. From an original focus on remittance agencies to facilitate fraudulent transactions, attention is now placed on the recruitment of money mules to facilitate these transactions. In many cases, the money mule is a victim themselves, and do not always realise the nature of their actions or the potentially criminal consequences they can incur.

There is opportunity for the banking and finance sector to assist in this space. These agencies are often unwittingly facilitating fraudulent transactions. It is difficult to balance convenience with security around financial transactions. The ability to instantaneously transfer funds overseas is a benefit to many legitimate consumers but is also drives change and innovation in offenders. It further makes it difficult for victims to identify or recover any lost funds.

A revised AICES can acknowledge the benefits of technology innovation across many sectors as they relate to cybersecurity and cybercrime. However, there is a corresponding responsibility to acknowledge the potential for change and disruption to criminal offending opportunities that are also brought forward with innovation. Many see only the positives of innovation through technology and are blind to the potential negatives that its use can bring until it is too late. This needs to be achieved through a combination of education and awareness targeted at potential victims as well as concrete steps at a system level to prevent and disrupt offending.

How should Australia pursue our cyber and critical technology interests internationally?

The current AICES places a strong emphasis on the need to collaborate internationally. This is a strength and should continue. In terms of fraud and related cybercrimes, collaboration is even more critical. The experiences of victims in Australia are largely similar to those in other countries. Notably, the challenges of responding to this type of victimisation is also consistent in a global context. This presents itself as a unique opportunity to work towards a shared goal in responding to cybercrime across all aspects of prevention, response, and support.

A revised AICES can provide a platform which articulates the need for collaboration and shared understandings in this area and gives legitimacy to much needed discussions on these topics. This is particularly the case for responding to victimisation and supporting those who have experienced victimisation.

How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?

The above notes the importance of collaboration at all levels. There is also a need to drive collaboration across sectors. In my experience, there has always been a desire to work together to tackle the many problems and challenges associated with fraud (and cybercrime as a whole). The stumbling block for many has been a lack of a framework to achieve this and competing interests. There is a need to articulate clear goals and objectives which can be agreed upon from all sectors. I would argue that this needs to focus on the victims themselves, and all work should keep this victim perspective in mind. Framing this within a human context should be the driving approach to generate real and concrete change in how government and all other sectors respond to this problem.

The AICES could provide a platform in which to facilitate collaborative endeavours between these sectors, which are all focused on a shared understanding of the problem and outcomes that are agreeable to all involved.

What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

In the area of fraud, there is a global need to improve on how all agencies related to the "fraud justice network" interact with and respond to victims. I have witnessed a consistent steam of professionals who wish to do better, but are constrained by many factors including resources, knowledge, and political will (to name a few). Fraud and cybercrime victimisation are often perceived as an invisible crime type, which does not gain the public attention similar to other offence types (street crimes for example). There is a need to give visibility and voice to those who experience this crime type and recognise it for the actual level of harm that it induces.

There is potential to build upon some of the work that has been done in the UK, US, and Canada to support victims of fraud. The approach to recognising the effects of victimisation is more pronounced in these countries, and while not perfect, provides a starting point. There is currently a dearth of support services available in Australia to assist with the support and recovery of fraud (and cybercrime) victims, at both an individual and a SME (small and medium enterprise) level. iDCare is the notable exception to this (it is a victim support centre established to assist those who experience identity crime, across Australia and New Zealand). The research establishes that those who have been successfully targeted once are more likely to experience revictimization. This is a cycle that needs immediate intervention to reduce the impacts and likelihood of continued victimisation and ongoing harms.

Key points related to the above submission

The above answers seek to bring to the forefront the need to recognise victims in any policy on cybersecurity and cybercrime. Victimisation across these fronts continues to rise not only in Australia, but globally. In 2018, the Australian Competition and Consumer Commission reported that Australians lost AUD$489.7 million to fraud. This figure has risen every year for the past decade and is projected to rise for 2019 and beyond. Given the known underreporting of fraud this figure is likely to represent only a minority of actual losses. Further, this does not capture the non-financial harms associated with victimisation.

Despite the magnitude of losses, there is a distinct lack of recognition of fraud victims and an inability to respond to these individuals in an appropriate manner. There is a dearth of support

services available to assist in the recovery (both financial and otherwise) of these victims. Too often, they suffer in silence, unable to disclose to anyone based on a sense of shame and a fear of reprisal from others. For those who do attempt to report, they are often met with direct victim blaming attitudes that denigrate them and their lived experiences. Further, there is little chance of obtaining any investigation into the offence and even less likelihood of recovering any funds lost. To exacerbate this, there is minimal support available to assist with, and promote recovery. The situation for many fraud victims can be dire, and it is not uncommon for individuals to experience varying levels of depression, with some explicitly contemplating taking their own lives. In some cases, victims have committed suicide, believing this was the only option available to them in response to what occurred.

Overall, the evidence points to the potential severity of impacts derived from fraud victimisation. It further points to the need to aid the many thousands of Australians who find themselves victims of cybercrime or a cybersecurity incident that threatens their livelihood and overall wellbeing. Despite this knowledge, there is currently a lack of recognition and voice of these victims across policy targeted at cybersecurity and cybercrime. This must change into the future.

A revised AICES can give a voice and legitimacy to the experience of individuals in Australia who suffer because of a cybersecurity incident or cybercrime victimisation. It is important for this group to be acknowledged, but it is also critical for other agencies to recognise the effects of their interactions and communications with victims. In many cases, it is the system and not the individuals who constrain the type of response (if any) offered to those in these circumstances.

I implore consideration of a victim perspective, and the acknowledgment of the inevitability of victimisation to be included constructively in a revised AICES. While much has been achieved in the area to date, there many opportunities for improvement regarding cybersecurity and cybercrime into the future. A wider recognition of the need to not only focus on prevention, but to also include the response to, and support of, victims is a crucial step in moving forward in this area.

I thank you for your consideration of this submission.

References

The following is a list of selected publications which expand upon and support my arguments in this submission. I can provide these (and others) in full text upon request.

Cross, C. (2019) 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminology and Criminal Justice Online first, 13 March.

Cross, C. (2019). Online Fraud. In Oxford Research Encyclopedia of Criminology and Criminal Justice. Oxford University Press. doi:10.1093/acrefore/9780190264079.013.488.

Cross, C. (2019) Reflections on the reporting of fraud in Australia. Policing: An International Journal. Online first: Doi: 10.1108/PIJPSM-08-2019-0134.

Cross, C. (2019) Responding to individual fraud: perspectives of the 'Fraud Justice Network'. In Holt, T. and Leukfeldt, R. (eds). Understanding the Human Factor of Cybercrime. London, UK: Routledge.

Cross, C. (2019) Who is to blame? Exploring accountability in fraud victimisation. Journal of Criminological Research, Policy and Practice. Online first: Doi: 10.1108/JCRPP-07-2019-0054.

Cross, C. (2018) Denying victim status to online fraud victims: The challenges of being a "non-ideal victim". In Duggan, M. (ed.) Revisiting the Ideal Victim Concept. London: Policy Press, pp. 243-262.

Cross, C. (2018) (Mis)Understanding the Impact of Online Fraud: Implications for Victim Assistance Schemes. Victims and Offenders. Online first: Doi: 10.1080/15564886.2018.1474154.

Cross, C. (2018) Victims' motivations for reporting to the 'fraud justice network'. Police Practice and Research. 19(6): 550-564. Doi: 10.1080/15614263.2018.1507891.

Cross, C. and Blackshaw, D. (2015) "Improving the police response to online fraud." Policing: A Journal of Policy and Practice 9(2): 119-128.

Cross, C., Richards, K. and Smith, R.G. (2016) Improving responses to online fraud victims: An examination of reporting and support Final Report. Criminology Research Grants: Canberra A.C.T.

Cross, C., Richards, K, and Smith, R.G. (2016) The reporting experiences and support needs of victims of online fraud. Trends and Issues in Crime and Criminal Justice 518: 1-14.

Cross, C., Smith, R. And Richards, K. (2014) Challenges of responding to online fraud victimisation in Australia. Trends and Issues in Crime and Criminal Justice 474: 1-7.