International Justice Mission Submission

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Introduction

International Justice Mission (IJM) is a global organisation that protects people in poverty from violence. We partner with local authorities in 33 projects across 19 countries to combat slavery, violence against women and children, and police abuse of power against people living in poverty.

As part of our work countering cross-border trafficking in Southeast Asia, IJM has had the honour to help remove, care for, and/or support victim identification for over 500 individuals whom we determined to be victims of trafficking into forced criminality ('forced scamming') within scam compounds. We also assisted in the legal process that led to the conviction of 15 perpetrators involved in trafficking persons into online scam operations.

Forced scamming is one of the most complex and fastest growing forms of modern slavery in the world. This is a global crime that needs an urgent global response to enforce laws on behalf of people being enslaved.

Likely, hundreds of thousands of people from at least 60 countries around the world are being exploited in the scamming compounds in Cambodia, Myanmar and Lao PDR.[1] An estimated 220,000 people are engaged in online scamming in Cambodia and Myanmar,[2] and approximately 85,000 people are being held in online scam centres in Lao PDR.[3]

IJM is committed to developing the capacity of local justice system actors to effectively identify victims as a key part of our mission to help governments protect people from violence. IJM offices in Cambodia, Thailand, the Philippines, Indonesia and Malaysia proactively coordinate with their government agencies and diplomatic missions to help facilitate rescues and repatriation of the victims and connect with government and non-government partners to provide legal and psychosocial support.

IJM believes that criminal accountability for forced scamming operators is essential to combat this growing transnational crime, and we hope to work with government agencies to eradicate this form of violent financially-motivated crime. Eradicating this crime will be difficult. It is highly lucrative and relatively straightforward for criminal networks to operate in unstable contexts. Governments can, however, impede and disrupt its growth, and care for survivors.

---

[1] USIP Senior Study Group Final Report. (May 2024). *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*. Available from: https://www.asienhaus.de/archiv/user_upload/ssg_transnational-crime-southeast-asia.pdf Page 8.

[2] UN Human Rights Office of the High Commissioner (Aug 2023). *Online Scam Operations and Trafficking into Forced Criminality in southeast Asia: Recommendations for a Human Rights Response*. Available from: https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

[3] USIP Senior Study Group Final Report. (May 2024). *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*. Available from: https://www.asienhaus.de/archiv/user_upload/ssg_transnational-crime-southeast-asia.pdf

Shield 6 – Strong region and global leadership

46. Do you view attributions, advisories and sanctions as effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

The illicit scam industry continues to operate and abuse trafficking and fraud victims with impunity because it is incredibly lucrative and there remains low risk of accountability for perpetrators. Diplomatic support and pressure from the Australian Government is critical to support meaningful local government law enforcement efforts.

IJM recommends the Australian Government pursue transnational accountability for elite scamming perpetrators, particularly through targeted individual sanctions**.** Australia should also:

- Empower AUSTRAC to identify and freeze Australian based assets linked to complicit scamming elites.
- Ban and proactively monitor for additional property purchases in Australia or business interests by foreign nationals linked to the scam industry.
- Re-think "capacity building" efforts to compromised regimes, where the problem is political will, not capacity. Addressing political will requires diplomatic support and pressure.

Corruption is a significant problem, but the U.S. Treasury Department's sanctioning in 2024 of Cambodian senator and business tycoon Ly Yong Phat and his resort and hotel business conglomerate was a good start, as well as U.S. Treasury sanctions in May 2025 of Saw Chit Thu, commander of the Karen National Army, which controls large portions of Myawaddy in Myanmar. IJM encourages Australia to join these efforts.

The locations of scam compounds are known, and the crime is dependent on access to the internet**.** This combination should provide multiple solutions for local authorities to directly combat this problem at the source.

For example, the Thai government's decisive action by focusing attention on the scam compounds, including cutting off the supply of Thai-side electricity and internet to the compounds in Myanmar in February 2025, should be publicly commended. Further, the Thai government must be urged to maintain the electricity and internet cuts and expand enforcement to include likely illegal internet connections, including the use of internet signal repeaters along the border. These actions will strengthen Thailand's commitment to cracking down on the criminal scam syndicates that have been operating with impunity for too long.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

Improve Victim Screening and Identification for Trafficked Workers

Local authorities in transit and destination countries continue to focus more on combatting cyber-enabled scams and fraud than on protecting trafficking victims, acquiring useful intelligence from their cooperation, or countering the human trafficking element of these cyber-enabled crimes. This leads to governments missing out on a substantial amount of information and intelligence needed for investigations by law enforcement and financial regulators.

Victim identification remains a major challenge for many Southeast Asian nations but is crucial to holding perpetrators accountable and stopping scams at the source. The 2024 Trafficking in Persons report[4] noted that many Thai and Indonesian officials lacked an understanding of human trafficking and could not effectively implement identification procedures consistently nationally, often resulting in authorities likely inappropriately arresting, penalising and deporting trafficking victims for illegal acts committed as a direct result of being trafficked.

The Australian Government has a key role to play in encouraging proper victim identification for trafficked workers followed by law enforcement action, and coordinating efforts across the region to gather intel from scam centre workers so that cyber security efforts and capacity building is relevant and current as tactics and techniques used by organised crime who run these scam centres evolves.

Australia should continue to promote the Non-Punishment Principle in regional forums such as ASEAN or Bali Process.[5] Disambiguating between criminals with agency and forced victims is critical. The current approach by many local authorities that involves numerous arrests, charges and convictions or fines and deportations of working-level scam centre foreign workers, rather than focusing efforts on scam managers, syndicates, and complicit officials, will do little to disrupt the illicit industry. Rather, it will likely re-victimise large numbers of trafficking victims forced to engage in criminal activity against their will, while leaving complicit officials in local areas and scam centre bosses untouched.

Improving forced scamming trafficking victim screening and identification will assist with the application of the Non-Punishment Principle for victims of trafficking and increase information for countries like Australia to use to disrupt scam operations.

Raise Awareness of Trafficking Risks for At-risk Populations

There is a focus within the Horizon 2 discussion paper on enhancing support for domestic victims of cybercrime and scaling victim support and systemic protections. Alongside these

---

[4] United States Department of State (June 2024). *Trafficking in Persons Report*. Available from: https://www.state.gov/reports/2024-trafficking-in-persons-report/

[5] ASEAN-ACT (May 2025) *ASEAN Guidelines on the Implementation of the Non-Punishment Principle for Protection of Victims of Trafficking in Persons.* Available from: https://www.aseanact.org/resources/asean-guideline-npp/

funded initiatives (e.g. 2024 Cyber Security Awareness Support for Vulnerable Groups grants program), the Government should consider funding NGOs or other community based groups in Southeast Asia who can share intelligence with law enforcement based on the cases they are working on. These groups can also undertake awareness raising initiatives in the region to stem the workforce fuelling online scam centres, as vulnerable migrant workers are often deceived by the false promise of legitimate work and are then then trafficked into scam centres.

IJM is currently partnering with the Mekong Club with funding from the U.S. Department of State Office to Monitor and Combat Trafficking in Persons to equip key businesses, including from the technology, social media and financial services sectors, to detect and respond more effectively to forced scamming.

Fraudulent job ads on social media have been an effective gateway for migrant jobseekers to be trafficked into scamming operations when applying for what they think are legitimate job offers in overseas companies – usually in IT or sales roles. Applicants are recruited through these fraudulent job advertisements through convincing recruitment processes and trafficked across country borders where oftentimes their passports are confiscated and they are subjected to debt bondage, surveillance and human rights abuses included violent punishments for underperformance or attempts to leave.

Due to our ongoing close cooperation and engagement, a major social media company has made IJM one of their trusted partners, along with other NGOs focused on forced labour in the region. Because of this relationship, when IJM identifies a likely fraudulent job ad, we inform the social media company, and they prioritise its review. Normally this would take days or weeks, but this partnership expedites the process.

Social media companies are aware of the problem of fraudulent job ads on their platforms, but they do not routinely post warnings about the existence of false job ads, and they often do not independently identify and remove these ads. While the private sector and governments have become more aware of cyber scam operations, a coordinated multi-stakeholder approach to combating this crime is still absent.

Strengthen survivor services

The scale and direction of human trafficking flows globally resulting from this crime type is unprecedented. As such, the infrastructure and capacity to care for victims is overwhelmed and under-resourced in source, transit and destination countries. Without support for survivors, critical information and collaboration with law enforcement necessary to stop trafficking and crime networks are being lost.

Local governments must increase funding for their social service agencies supporting victim services and strengthen processes for repatriation, and where local governments lack budgets, donor governments should consider supporting frontline efforts by local governments and NGOs.

Elevate survivor voices

The voices of survivors of trafficking into forced scamming should be elevated through engagement with governments, directly in cases or intelligence gathering but also publicly in appropriate forums to increase government support and pressure for increased law enforcement efforts and survivor services and protection.

IJM is strengthening efforts of local and global survivor leader groups, including "The Future Will be Better" in Thailand, which brings together forced criminality/forced scamming survivors who voluntarily join to process and overcome their trauma and advocate for protection for others vulnerable to trafficking for forced scamming, especially through the power of storytelling. Contact International Justice Mission Australia to explore how to engage with this local survivor group.

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

Due to the scale of illicit economies forced scamming is fuelling, Australia should place online fraud/scamming on the agenda of major economic forums like APEC and the East Asia Summit to build consensus for action to address the root causes of the cybersecurity threats we face in the region, which are directly affecting the economic interests of Australians.

Through the Mekong-Australia Program (MAP) on Transnational Crime, DFAT should fund Australian law enforcement, security and border protection agencies to work with their counterparts in Mekong countries who are committed to curtailing scamming operations including by conducting joint operations, sharing information, and undertaking capacity building exercises. To date there has been limited MAP programming directly addressing trafficking into scam compounds, creating an opportunity for Australia to lead. Leveraging MAP's transnational crime pillar, new initiatives could focus on strengthening cross-border referral pathways for scam victims, embedding survivor-informed victim identification training, and resourcing coordinated investigations that target scam syndicates and complicit officials.

Whilst the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime already has a focus on addressing forced scamming through the Adelaide Strategy for Cooperation, practical operationalisation of stated objectives should be prioritised. For example, Australia could use its co-chair role to push for concrete actions, such as joint law enforcement operations, intelligence-sharing mechanisms, and the adoption of ASEAN's Non-Punishment Principle guideline to ensure victims trafficked into scam compounds are protected rather than penalised.

The ASEAN-Australia Comprehensive Strategic Partnership focuses on strengthening justice systems to ensure just punishment of traffickers and protection of the rights of victims. Australia should prioritise deepening cooperation in preventing and combating transnational crime on issues of common interest.

Conclusion

International Justice Mission appreciates the opportunity to make a submission relating to Shield 6 of the discussion paper to develop Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

Should you wish to discuss any aspects of this submission, please contact IJM Australia [redacted]