Assistant Secretary Michael George DeSombre
for the Bureau of East Asian and Pacific Affairs (EAP)
Hearing with the Senate Foreign Relations Committee on
"Protecting Americans from Global Scam Operations:
Assessing the U.S. Response"
Written Testimony
August 6, 2026

Chairman Risch, Ranking Member Shaheen, and distinguished Members of the Committee, thank you for the opportunity to testify on "Protecting Americans from Global Scam Operations" and, specifically, on how the Department is countering criminal online scams in the East Asia and Pacific region.

Criminal scams targeting Americans are a global problem, and in Burma, Cambodia, and Laos, criminal scam operations have industrialized at an unprecedented scale. What began as isolated fraud rings have transformed into a sprawling illicit economy, run out of compounds that are guarded, self-contained, and staffed with an increasingly professionalized and sometimes coerced workforce. Credible U.S. and international sources report individuals from dozens of countries are exploited through human trafficking to work at online scamming operations, with victims of forced criminality in scam centers across these three countries alone potentially numbering in the hundreds of thousands each year. This is not a patchwork of isolated criminal enterprises—it is an industry, complete with its own infrastructure, labor force, and supply chains.

U.S. government reporting and international experts share the same assessment: Chinese-origin transnational criminal organizations are the major force driving the scam economy in Southeast Asia and globally. In nearly every case, the leadership of these scam centers and transnational criminal organizations is composed of Chinese nationals. U.S. citizens have become significant targets. Our initial 2025 estimate placed reported losses from Southeast Asia-based scam groups at $12.5 billion—a conservative figure. As our analysis nears completion, we anticipate actual losses to be significantly higher.

It is estimated that these groups inflicted up to $114 billion in losses on East Asia and Pacific countries in 2025. As we apply pressure to disrupt them in one location, we have seen them move to other locations and adapt their business model to scale down their physical footprint but sustain the intensity of their scamming with technology. In Cambodia, for example, we have seen some compounds closed by police raids relocate operations elsewhere in the country.

The Department of State's strategy, in line with the President's March 6 Executive Order, is to identify vulnerabilities across the transnational criminal organizations and apply sustained pressure at scale to disrupt their criminal actions and impose costs on the organizations. That includes going after the bosses and financiers of the criminal organizations in addition to disrupting their physical and digital infrastructure, financial flows, and communications networks. Dismantling leadership and cutting off financing is one of the critical ways to break the criminal networks rather than merely temporarily disrupt them.

On March 6, 2026, President Trump signed Executive Order 14390 to make clear our focus is to dismantle and degrade the transnational criminal organizations behind this threat. The Executive Order directs the Secretaries of State, Treasury, War, and Homeland Security, and the Attorney General, to develop an Action Plan to identify, disrupt, and dismantle these networks. The scale demands nothing less, with harm in 2025 triple to that of 2023 and thousands of Americans targeted from all 50 states. My INL colleague David Bedard will detail the interagency and State Department-focused Action Plans.

Across the region, our diplomacy carries one consistent message, repeated in every capital: countries must go after transnational criminal organization bosses, not just low-level operations, and work to dismantle the entire scam ecosystem. We are raising this issue directly and repeatedly with Cambodia, Burma, and Laos, and with every regional partner whose cooperation we need. We are also raising this issue directly with China and have encouraged them to demonstrate that they are not abetting these actions by allowing Chinese crime bosses to be held accountable internationally.

Our message to all of these governments is simple: we must drive up costs for the transnational criminal organizations, restrict their access to victims, and make clear that no safe-haven jurisdiction can shield them from the reach of the United States.

We have backed this message with action. On July 23, Secretary Rubio announced the creation of a new visa restriction policy aimed at targeting individuals involved in cybercrime and cyber-enabled crime, including scam centers and sextortion. We aim to utilize this policy to the greatest extent possible. In 2025, a Section 311 rule cut off Huione Group's access to U.S. dollar accounts. Separately, sanctions and U.S. law enforcement action against the Prince Group transnational criminal organization was the first domino in the international takedown of the organization, its CEO Chen Zhi, and over 140 of its affiliates. Chen Zhi, in particular, was also the target of a DOJ indictment and an approximately $15 billion cryptocurrency forfeiture, the largest in history. On April 23, Treasury sanctioned Cambodian Senator Kok An and 28 additional individuals and entities. In April 2026, the Department of Justice’s Scam Center Strike Force charged two Chinese nationals tied to a Burma-based scam center targeting Americans and froze over $700 million in cryptocurrency.

In partnership with INL, in April, I led the launch of a 13-country diplomatic coalition of U.S. allies and partners—countries most affected by the scam threat and most capable of joining us in action against it. That Counter-Scams Contact Group includes Australia, Canada, Indonesia, Japan, Malaysia, New Zealand, the Philippines, the Republic of Korea, Singapore, Thailand, the United Kingdom, and Vietnam. We are using this grouping to rally support for going on offense, in line with U.S. policy direction under the Executive Order, and to build a diplomatic framework for closer alignment on law enforcement action, asset seizures, financial sanctions, diplomatic pressure, and information-sharing. It also signals our continued commitment to reaffirming U.S. leadership in the region.

This threat originates abroad and is putting tens of thousands of Americans and their livelihoods at risk across all fifty states. It is a credit to the Committee that you have elevated attention—including through the bipartisan SCAM Act—on the need to fight back against the criminal groups using these scams to harm our fellow citizens. As part of the whole of government effort driven by the President's March 6 E.O., the Department of State will continue to do all we can, including in East Asia and the Pacific region, to raise the cost on the criminal scam groups and drive down the harm done to Americans.

Thank you, and I welcome your questions.