U.S. Congress Joint Economic Committee
Hearing on
The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters

Testimony of Stewart Baker
March 25, 2026

It is a pleasure to appear before you to support greater authority for the private sector to fight cybercrime. Although I have served several tours in government, most recently as assistant secretary for policy at the Department of Homeland Security and general counsel of the National Security Agency, I believe that we rely too heavily on government for defense against cybercrime. I'm a long-time advocate for giving more authority to the private sector; my public record on the topic dates back at least to 2012, when I debated "hacking back" with Prof. Orin Kerr.

I have two preliminary observations about this topic. First, government officials almost without exception insist that empowering the private sector is dangerous and unnecessary. They claim that only government officials can handle law enforcement responsibilities and that empowering private actors in this sphere will lead to "vigilante justice." This is just wrong. Cybercrimes, including cyberscams, have exploded in recent years. And, good as they are on an individual basis, U.S. law enforcement agents have not been able to keep up. The anonymous and international nature of these crimes requires a far more innovative and aggressive response than government has been able to muster. When it rejects what it calls vigilante justice, the government too often offers victims no justice at all.

This is wrong. By pretending that those are our only choices, the government is ignoring the many ways in which the energy and creativity of the private sector can be prudently harnessed to help victims of crime. In fact, the United States has a long history of doing exactly that. Our legal system allows the private sector to take on traditional government responsibilities in a wide variety of law enforcement contexts. These roles are not controversial because they've been around for decades, if not centuries. To pick a few examples, stores and event locations routinely hire private security guards, who often carry weapons and have authority to detain lawbreakers for prosecution. Bail bondsmen hire private bounty hunters to track down suspects who skip town after posting bail. Family members grieving over a crime may hire private investigators to do what local police lack the resources to accomplish. Private citizens who spot violations of government contract law can file a "qui tam" lawsuit against the violator in the government's name. In the case of

many other crimes, private citizens can gather evidence, report the wrongdoing, and claim a portion of what the government recovers at the end of the day.

None of these delegations to the private sector has resulted in vigilante justice. That's because in each case the additional authority comes with limits, and additional government oversight, to avoid abuses.

For some reason, however, as technology has enabled new crimes and created new victims, the government has been strikingly reluctant to consider new solutions that include private action. So I'm delighted that the Joint Committee has called this hearing to consider new approaches. Instead of rejecting private sector action out of hand, the government should be talking about ways to unlock private resources while also building safeguards against abuse. Chairman Schweikert's recent bill, the Scam Farms Marque and Reprisal Authorization Act, H.R. 4988, is a valuable contribution to that discussion.

H.R. 4988 authorizes private parties to find and seize the property of individuals and foreign governments who are involved in cybercrime and have committed an act of aggression against the United States. Seizing the proceeds of crime is a well-established criminal enforcement tool, and the U.S. has procedures for sharing seized assets with private parties who provide information or other assistance that contributes to the seizure. H.R. 4988 goes a step further, allowing private sector entities to initiate the seizure, with safeguards:

- Both the private party authorized to carry out the seizure and the target of the seizure must be designated by the government, a provision that helps prevent irresponsible seizures.
- In addition, the bill authorizes the President to issue further instructions limiting the scope of the private actor's discretion.
- Recipients of such an authorization must post a security bond to ensure compliance with the terms and conditions specified by the President.

This structure allows the government to exercise substantial control over the actions of any private parties who receive such a letter.

I see one significant risk in the structure. It seems to authorize parties to seize and keep 100% of the assets of a designated target. But not all assets held by criminals are the fruits of their crime. And, more importantly, the assets held by cybercriminals were usually taken from innocent victims. Justice is not done by transferring all of those assets to a third party. Instead, those victimized by the target should have an opportunity to reclaim at least a portion their property. The private parties who perform the essential service of recovering that property should be rewarded, but that reward should be limited to a substantial

fraction, up to 25 or 30 percent, of what they recover, and the remainder should go back to any victims who can prove their claim. This is consistent with the most generous awards given under U.S. law to whistleblowers who provide critical assistance when the government imposes a fine or conducts a seizure a domestic context.

As I see it, using letters of marque to pursue criminal assets has one principal advantage over relying on law enforcement. It is this. The assets of cybercriminals are likely to be well hidden from governments, but hiding those assets requires the services of many intermediaries. The intermediaries are likely criminals themselves, and they are unlikely to ruin their business by talking to the U.S. government. Unless they stand to gain a substantial award. Letters of marque are a way of offering such an award, while also allowing the government to vet the recipients to avoid making payments to those who don't deserve them.

I do not suggest that the bill is perfect. If I were drafting it, I would be more explicit about the President's authority to impose terms and conditions on holders of letters of marque. A representative list of such conditions might include limitations on the methods used to seize funds, rules about when seizures in violation of foreign law are permitted, and express government authority to revoke a letter of marque or otherwise penalize holders who exceed their authority. Similarly, holders of letters of marque might be required to obtain specific approval for seizures of assets in the hands of a foreign government. The U.S. may have very different views about seizures from a government depending on the government. Targeting North Korea's organized cryptocurrency thieves is one thing; targeting a government with which U.S. relations are more complicated is another.

If the committee sees the value in awarding a portion of seized criminal assets, I would urge it to look beyond letters of marque to reform of the current rules for making awards from law enforcement proceeds. Frankly, those rules are a mess. Some agencies, such as the SEC, the CFTC, and Treasury's FinCEN, have embraced whistleblower awards of ten to 30 percent with enthusiasm. For timely, original, and credible information leading to a successful enforcement action, the SEC typically awards 10 to 30 percent of what it collects from wrongdoers; its largest award so far is nearly $279 million. The CFTC's top award was $200 million in 2021.

In contrast, the law governing Justice Department awards is remarkably stingy. By law, the top award from seized assets in the Justice Department's asset forfeiture fund is $250 thousand if approved by the Deputy Attorney General. It can go to $500 thousand if approved by the Attorney General, but that's the maximum. 28 USC 524(c)(J)(2). To achieve its goals H.R. 4988 will need to override these limits for holders of letters of marque. Indeed, in light of the widespread standardization of other government awards around ten

to thirty percent without arbitrary limits, Congress should authorize 10-30% awards from the forfeiture fund, at least where there is no doubt about the value of the claimant's contribution to the success of the seizure.

Finally, although it is probably outside the scope of H.R. 4988, I would urge the Committee to look at other ways to enable more aggressive private defense of computer networks. As things stand today, large sums, innovative technology, and lots of private talent are all focused on defending corporate networks against attackers, *once they get inside the network*. Taking any action outside the network to stop attackers is presumptively illegal under the Computer Fraud and Abuse Act. Only government law enforcement can operate there. But the government's resources are far more limited than those available to private enterprise. And even with large budgets, law enforcement cannot provide seamless defense because it lacks access and insight into what's happening inside corporate networks. To give one example, attackers often spend days or weeks inside a victim network, assembling the files they want to steal. Then, usually on a long weekend, they may exfiltrate the data to a password protected site that they control. Using its network monitoring tools, the victim will know within seconds that the data has been stolen, where it's been sent, and even what the password is for that site. In a rational world, we'd defeat the theft in a few seconds by using the password to log onto the criminal site and remove or encrypt the stolen data. That's a defensive action that could easily be automated. In the real world, however, that will never happen, because running the rescue program would be a felony. The FBI could do it, but not in seconds, or minutes, or even, really, days. Only the company that owns the network has the information needed to deploy such a system quickly; the law should not make that impossible.

I offer this example not because it is the only, or the most important, defensive tactic that is being thwarted by the strict line drawn between lawful "inside" defenses and unlawful "outside" defense. I offer it because it shows that the Justice Department should be doing more to approve defensive actions outside the victim's corporate network. As with all such private remedies, the government would have to impose guardrails to avoid abuse, but that should not be a reason to do nothing.

Whatever the outcome, I appreciate the fact that H.R. 4988 and this hearing have again opened the door to a debate over how private enterprise can supplement law enforcement's efforts to deter cybercrime. There is much opportunity for progress in this field if we can get beyond slogans like "vigilante justice" and ask instead who can do the best job of protecting against cybercrime and what rules would make that possible.

Thank you for your attention.