BANK POLICY INSTITUTE

The Same Team – Changing How Government and Industry Protect Against Cyber Threats

By Chris Feeney

March 10, 2020

If a hostile army were to storm our shores, the U.S. military would be there, quickly mobilized and deployed to meet the threat. After all, providing for the common defense is one of the most fundamental roles of government. In reality, however, our nation is assaulted by hostile armies every day. They are not storming our beaches, but our networks and our servers. Our critical infrastructure, the majority of which is owned by private industry, is at risk from a host of adversaries ranging from hostile nation-states to rogue criminal groups.

Private industry — including energy companies, telecommunications providers and financial services firms — are essential for the functioning of our society. They operate communications systems like mobile services, the Internet and the ability to dial 911; they ensure the power is on and that gas stations have fuel; and they allow you to make payments and provide loans to help businesses operate and grow. Our reliance on these services, and the chaos that would ensue if one of them failed to function, make these industries prime targets for our nation's adversaries. It's the reason financial firms invest billions of dollars each year into their own cybersecurity and cyber resiliency, as well as collective initiatives like the Financial Services Intelligence Sharing and Analysis Center, the Financial Systemic Analysis and Resilience Center, fTLD Registry Services and Sheltered Harbor.

Despite these investments, there are limits to the private sector's ability to protect our critical infrastructure. The best way to ensure the continuity of operations for these entities is for the government to treat private sector entities as partners who share the same mission to defend against threats and preserve our way of life.

Today, public-private partnerships have many important building blocks in place, but current mechanisms are limited, and we are missing critical opportunities to share timely and usable information. The financial sector has identified several important steps that government should take to strengthen our cybersecurity and protect our critical infrastructure:

- Designate critical infrastructure a formal customer of the intelligence community, prioritizing collection, analysis and timely information sharing;
- Expand and make permanent the Cybersecurity Information Sharing Act's legal protections for sharing cyber threat information;
- Establish a national cybersecurity director in the White House; and
- Strengthen the role of sector-specific agencies (e.g. Department of Treasury, Department of Energy) responsible for coordinating with private sector entities on preparedness, response, mitigation, recovery and the overall resilience of critical infrastructure.

Thankfully, the need to treat critical infrastructure as a core partner is being recognized more widely. The recently updated National Counterintelligence Strategy highlighted the need for the government to prioritize the protection of critical infrastructure. It discusses a "whole of society" approach to encourage better public-private collaboration and marks an important expansion in the federal government's counterintelligence mission. The strategy's five pillars — protect the nation's critical infrastructure, reduce threats to key U.S. supply chains, counter the exploitation of the U.S. economy, defend American democracy against foreign influence, and counter foreign intelligence cyber and technical

operations — reflect the reality of today's threat environment in which increasingly sophisticated capabilities are being deployed and commercialized by threat actors.

In his announcement of the new strategy, National Counterintelligence and Security Center Director William Evanina stressed the need to provide actionable information to private firms so they can improve their defenses in a rapidly changing threat landscape. The strategy echoes statements from the Cybersecurity and Infrastructure Security Agency and the National Security Agency, both of which have pledged to share more information with private industry.

These are positive steps but Congress also has a role to play. The Cyberspace Solarium Commission, created by the National Defense Authorization Act will present its report to Congress on March 11th along with a set of legislative recommendations. The Commission is charged with developing a strategic approach to defending the U.S. in cyberspace and will release 75 recommendations covering areas such as government structure and organization, promoting national resilience, and operationalizing collaboration with the private sector.

The Commission, to its credit, has conducted extensive engagement with critical infrastructure including ongoing dialog regarding key challenges, opportunities to address them, and has recognized the limitations of our current collaboration model. For example, while the government and industry have mechanisms in place to share cyber threat indicators, this information is limited, not actionable, and not in real-time. For advanced critical infrastructure sectors like financial services, telecommunications and energy, the Commission recognizes the need for deeper, more sophisticated collaboration between our respective intelligence professionals around critical vulnerabilities and points of failure. With a common understanding of what is most important to protect, the federal government and the financial services industry can better inform national intelligence collection and analysis priorities, ensure timely sharing of actionable information, and allocate resources accordingly.

When the Commission releases its report, we look forward to working with Congress to pass legislation to address these gaps and better protect our nation. As our cyber adversaries continue to grow in size and sophistication, both government and critical infrastructure will benefit from greater collaboration. We share the same goals and, most importantly, are on the same team.