Cybersecurity Issue Summary

Banks are increasingly under cyber attack by foreign nations and criminal groups seeking to disrupt the financial system and undermine the functioning of the U.S. economy. Banks and other financial institutions have a long history of working across the industry and with government partners to protect firms and the U.S. economy against threats. The financial sector was the first to form an information sharing and analysis center in 1999 and established a strong sector coordinating council in 2002 – both of which have served as leading examples other critical infrastructure sectors have sought to replicate.

As cyber threats continue to grow in scale and sophistication, the ability of banks to protect themselves and the broader financial system would benefit from enhanced information sharing and a more collaborative relationship with the nation's intelligence community. The ability of industry threat experts to work with intelligence agencies to refine collection, analysis, and subsequent information sharing would address critical gaps in the financial sector's ability to defend the financial systems Americans count on for every day life.

BPI's Position

Despite the existing framework for public-private partnerships, current information sharing mechanisms are limited, and we miss critical opportunities to share timely and usable information. The best way to ensure the continuity of operations for critical infrastructure entities such as financial institutions, telecommunications and energy providers, 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. The recently updated National Counterintelligence Strategy highlighted the need for a new approach and includes protecting critical infrastructure as one of its core pillars for defending the U.S. against adversaries.

Recommendations:

The financial sector has identified several important steps that Congress and the executive branch could take to strengthen our cybersecurity and protect our critical infrastructure.

- Congress should designate critical infrastructure a formal customer of the intelligence community, prioritizing collection, analysis and timely information sharing (this requires legislative action)
- Congress should expand and make permanent the Cybersecurity Information Sharing Act's (CISA) legal protections for sharing cyber threat information (currently set to expire in 2025)
- The Executive Branch should establish a national Cybersecurity Director in the White House

Cyberspace Solarium Commission

The Cyberspace Solarium Commission, created by the 2019 National Defense Authorization Act, released its report to Congress on March 11, 2020. The Commission was charged with developing a strategic approach to defending the U.S. in cyberspace and released more than 80 recommendations, including those listed above, covering areas such as government structure and organization, promoting national resilience, and operationalizing collaboration with the private sector. BPI looks forward to working with Congress to pass legislation to address gaps in our regulatory structure 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.