bpi BANK POLICY INSTITUTE

August 18, 2021

Information Sharing & Collaboration Issue Summary

Banks are increasingly under cyberattack 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.

While today sharing between the financial sector and the various US government entities is mostly one way, coming from the financial sector, there are numerous opportunities to move from the current sharing model to actual collaboration. The financial services sector is uniquely equipped with capabilities, depth, cleared personnel and a strong trust network to actively contribute to national security initiatives. Recent examples of lost opportunities to collaborate include the TrickBot takedown organized by Microsoft and FS-ISAC in 2020, and the ongoing DDoS extortion campaign in the sector, most visible in the shutdown of the New Zealand Stock Exchange. The NSA Cybersecurity Collaboration Center could be one venue for this enhanced two-way sharing activity, and the financial sector could add significant value to CISA's recently announced Joint Cyber Defense Collaborative. Below please find additional information on three of the primary information-sharing and collaboration mechanisms within the financial sector.

Background on Existing Information-Sharing Efforts

Financial Services Information Sharing and Analysis Center (FS-ISAC)

FS-ISAC, representing approximately 4,600 US financial institutions covering banks, credit unions, insurance companies, asset managers and payment processors, as well as FMI's such as stock exchanges, has numerous interfaces with the US government. FS-ISAC is a not-for-profit cybersecurity intelligence sharing organization that is governed by its members in the sector, and has been operating, as the first ISAC, for over 20 years. Its focus is on intelligence sharing and enrichment, both tactical and strategic. Today, under current regulations in the sector, it views incident notification as a member obligation separate from the sharing of actionable intelligence among members.

The two principal mechanisms for FS-ISAC to share information with the US government are via DHS/CISA and the U.S. Department of Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) as the Sector Risk Management Agency for the financial sector. Through CISA, FS-ISAC is able to share information among the participants at CISA Central, formerly known as the National Cybersecurity and Communications Integration Center (NCCIC) and is able to formally submit Requests for Information (RFIs) to support the financial sector's needs in dealing with a threat. RFIs typically do not generate actionable responses.

Through Treasury's OCCIP, FS-ISAC also shares information, submits RFIs and communicates priority areas of intelligence requirements for the protection of the sector. FS-ISAC also provides trends, issues and summary data to Financial and Banking Information Infrastructure Committee (FBIIC) partners to assist them in managing overall risk to the sector.

Sharing from the US government to the sector is mostly limited to the classified briefings that OCCIP holds monthly, and occasional Critical Infrastructure Sharing and Collaboration Program (CISCP - operating out of DHS/CISA) pre-notification of major releases. This early notification allows FS-ISAC to prepare data specifically for the sector and immediately release critical information in an actionable form that reaches operators minutes after the CISA release is public.

Analysis and Resilience Center for Systemic Risk (ARC)

The Analysis and Resilience Center for Systemic Risk (ARC) is a non-profit, cross-sector organization designed to mitigate systemic risk to the nation's most critical infrastructure from existing and emerging threats. ARC members are owners and operators of federally designated critical infrastructure which underpin economic and national security. The ARC facilitates operational collaboration between our members, the US government, and other key sector partners in a controlled environment where participants can securely collaborate. In conjunction with US government partners, participants identify risk gaps and collectively develop measures to increase the resilience of the critical system, asset, or function being examined. Examples of areas reviewed on a global basis include risks to the wholesale payments ecosystem and to securities settlement processes.

The ARC and its members:

- Share systemic risk priorities and resilience outcomes on financial services sector critical systems, assets, and functions with US government partners. A similar model is under development with US government partners for the energy sector.
- Work with US government partners to improve intelligence collection and reporting on activity potentially targeting critical systems, assets, or functions. This activity will soon include ARC member energy sector firms and the Department of Energy.

National Cyber-Forensics and Training Alliance (NCFTA)

The National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit partnership between industry, government, and academia established for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber-crime. The NCFTA operates in a concerted effort with partners by sharing real-time information and working as an early-warning system to pass information quickly to its members. Since its establishment in 2002, the NCFTA has prevented over $1 billion in potential losses while also helping to identify critical threats impacting private industry.

The NCFTA sharing model includes sharing with and supporting law enforcement to enable authorities to disrupt cyber-criminal actors and groups wherever they may be. Information sharing between the NCFTA community has led to several successful law enforcement investigations (find more information here). Through its partnership with many private-sector members, Carnegie Mellon University's CERT, and the FBI's Internet Crime Complaint Center (IC3), the free-flow exchange of threat intelligence assists investigation and prosecution of cyber criminals worldwide.