September 2020

CRITICAL INFRASTRUCTURE PROTECTION

Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts

GAO Highlights

Highlights of GAO-20-631, a report to Congressional Addressees

Why GAO Did This Study

For decades, the federal government has taken steps to protect the nation's critical infrastructures. The financial services sector's reliance on information technology makes it a leading target for cyber-based attacks. Recent high-profile breaches at commercial entities have heightened concerns that data are not being adequately protected.

Under the Comptroller General's authority, GAO initiated this review to (1) describe the key cyber-related risks facing the financial sector; (2) describe steps the financial services industry is taking to share information on and address risks to its sector; and (3) assess steps federal agencies are taking to enhance the security and resilience of the sector. GAO analyzed relevant reports and information to determine risks and mitigation efforts and compared agency efforts against federal policies and guidance. GAO also interviewed officials at 16 private sector entities, two self-regulatory organizations, and eight federal agencies, including the Department of the Treasury.

What GAO Recommends

GAO is making recommendations to Treasury to track and prioritize the sector's cyber risk mitigation efforts, and to update the sector's plan with metrics for measuring progress and information on how sector efforts will meet sector goals and requirements, including those contained within the *National Cyber Strategy Implementation Plan.* Treasury generally agreed with the recommendations.

View GAO-20-631. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Michael Clements at (202) 512-7763 or clementsm@gao.gov.

What GAO Found

The federal government has long identified the financial services sector as a critical component of the nation's infrastructure. The sector includes commercial banks, securities brokers and dealers, and providers of the key financial systems and services that support these functions. Altogether, the sector holds about $108 trillion in assets and faces a variety of cybersecurity-related risks. Key risks include (1) an increase in access to financial data through information technology service providers and supply chain partners; (2) a growth in sophistication of malware—software meant to do harm—and (3) an increase in interconnectivity via networks, the cloud, and mobile applications. Cyberattacks that exploit risks can occur against either public or private components of the sector. For example, in February 2016, hackers were able to install malware on the Bangladesh Central Bank's system through a service provider, which then directed the Federal Reserve Bank of New York to transfer money to accounts in other Asian countries. This attack resulted in the theft of approximately $81 million.

Several industry groups and firms are taking steps to enhance the security and resilience of the U.S. financial services sector through a broad range of cyber risk mitigation efforts. These efforts include coordinating within the sector through groups such as the Financial Services Sector Coordinating Council and the Financial Systemic Analysis and Resilience Center, conducting industrywide incident response exercises, sharing threat and vulnerability information, developing and providing guidance in conducting risk assessments, and offering cybersecurity-related training.

The Departments of Homeland Security and the Treasury and federal financial regulators are also taking multiple steps to support cybersecurity and resilience through risk mitigation efforts. Among other things, federal agencies provide cybersecurity expertise and conduct simulation exercises related to cyber incident response and recovery. Treasury, as the designated lead agency for the financial sector, plays a key role in supporting many of the efforts to enhance the sector's cybersecurity and resiliency. For example, Treasury's Assistant Secretary for Financial Institutions serves as the chair of the committee of government agencies with sector responsibilities, and Treasury coordinates federal agency efforts to improve the sector's cybersecurity and related communications.

However, Treasury does not track efforts or prioritize them according to goals established by the sector for enhancing cybersecurity and resiliency. Treasury also has not fully implemented GAO's previous recommendation to establish metrics related to the value and results of the sector's risk mitigation efforts. Further, the 2016 sector-specific plan, which is intended to direct sector activities, does not identify ways to measure sector progress and is out of date. Among other things, the sector-specific plan lacks information on sector-related requirements laid out in the 2019 *National Cyber Strategy Implementation Plan*. Unless more widespread and detailed tracking and prioritization of efforts occurs according to the goals laid out in the sector-specific plan, the sector could be insufficiently prepared to deal with cyber-related risks, such as those caused by increased access to data by third parties.