2024 U.S. Government Programs and Services for Financial Sector Security and Resiliency - Small to Mid-Size Institutions

In the 2023 National Cybersecurity Strategy, President Biden called for an increase in public-private collaboration to address the threats and risks in today's world through cutting edge approaches to information sharing and collaboration opportunities. Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) has developed this brochure to highlight new and unique programs and opportunities that are available to our small and mid-size financial sector partners. These opportunities look to enhance cybersecurity posture, information sharing, and resilience. This is not a comprehensive list of all programs and opportunities available. Please reach out to Treasury OCCIP or the listed POCs for each program for more information.

U.S. Treasury – Automated Threat Information Feed

Treasury's Automated Threat Information Feed is a public-private information sharing program that provides financial institutions with access to a tailored cyber threat feed. This feed, which is currently in a pilot phase, will aggregate indicators from Treasury, other U.S. Government entities, international partners, and participating financial institutions. Through OCCIP's partnership with the Pacific Northwest National Laboratory (PNNL), data from open sources and other PNNL holdings will also be made available through the feed. Financial institutions may choose to contribute data to the feed on a voluntary basis or use it as source of information on potential threats targeting the sector.

For more information on Treasury's Automated Threat Information Feed, or to inquire about participation, please contact OCCIP at (OCCIP-Coord@treasury.gov).

U.S. Treasury – Office of Intelligence and Analysis – T-Suite

The Treasury Cyber Collaboration Suite (T-Suite) in downtown D.C., located just a few blocks from the White House, was established in 2024 and is led by the Department of the Treasury's Office of Intelligence and Analysis (OIA). The T-Suite advances broad industry collaboration with intelligence professionals to identify and mitigate cyber threats identified in intelligence channels and by sector partners. The T-Suite links OIA, OCCIP, the Intelligence Community, and cleared industry representatives in one space to bolster tactical and strategic cooperation.

For more information on Treasury's T-Suite or to inquire about participation, please contact (OIA-Tsuite@treasury.gov).

Treasury's Office of Foreign Asset Control (OFAC) serves as the sanctions arm for Treasury. OFAC has developed sanctions that specifically target actors engaged in malicious cyber activities, including those intent on causing cyber harm to U.S. financial institutions. Additionally, the FBI is also heavily engaged in dismantling the infrastructure of global cyber criminals. If you have information about potential cyber-related sanctions violations or leads regarding persons engaged in malicious cyber activities that you would like to share with OFAC, please visit https://ofac.treasury.gov/contact-ofac to contact OFAC's Compliance Hotline.

Cybersecurity and Infrastructure Security Agency – Cyber Hygiene Program

CISA's Cyber Hygiene (CyHy) Vulnerability Scanning Services allows participating organizations to receive CISA conducted vulnerability scans on their internet-facing systems. These scans identify known exploited vulnerabilities (KEVs) and then provide actionable feedback to the organization. A separate Web Application Scanning Service identifies web application weaknesses related to the OWASP categories, broken access controls, security misconfigurations, and use of outdated protocols, software, and operating systems. Enrollees received individualized reports for each service that can aid awareness and decision-making. CISA also produces an aggregated and anonymized monthly Vulnerability Snapshot which illustrates trends, patterns, and common vulnerabilities discovered among enrolled financial services sector members.

Membership in the program is free and is open to any critical infrastructure entity. For more information on the CISA CyHy Vulnerability Scanning Services please visit https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning or email (vulnerability@cisa.dhs.gov).

In addition to the programs above, OCCIP's Cyber Intelligence and Risk Analysis (CIRA) team facilitates information sharing on cybersecurity threats and vulnerabilities within the U.S. financial sector. In addition, CIRA manages domestic partnerships among U.S. Government and private sector entities to enhance collective risk management. To receive CIRA original production reports and mitigation recommendations, please contact (OCCIP-Coord@treasury.gov).