Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Office of Foreign Assets Control Cyber-Related Sanctions Program Risk Management

The Federal Financial Institutions Examination Council (FFIEC) members[1] developed this statement to alert financial institutions to recent actions taken by the Department of Treasury's (Treasury) Office of Foreign Assets Control (OFAC) under OFAC's Cyber-Related Sanctions Program and to the potential impact that sanctions may have on financial institutions' operations, including the use of services of a sanctioned entity.

This statement is intended for information only and does not contain any new regulatory expectations. This statement highlights that compliance with OFAC sanctions can impact information technology and other operations. Additional information on requirements and expectations regarding OFAC-related compliance is available from OFAC. Institutions may refer to the FFIEC *Information Technology (IT) Examination Handbook* for additional information regarding operational risk management.

BACKGROUND

OFAC implemented the Cyber-Related Sanctions Program on April 1, 2015, in response to Executive Order 13694 and a related declaration of a national emergency to address the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States caused by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by, entities located, in whole or in substantial part, outside the United States.[2] Since the program's inception, OFAC has issued sanctions against entities who are responsible for, are complicit in, or that have engaged in, certain malicious cyber-enabled activities, including by providing material and technological support to malicious cyber actors that have targeted U.S. organizations. Some of the sanctioned entities claim that they are U.S.-

[1] The FFIEC comprises the principals of the following: the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

[2] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

based and offer services to financial institutions.[3] U.S. persons are generally prohibited from engaging in transactions[4] with sanctioned entities and all property and interests in property of the sanctioned entities subject to U.S. jurisdiction are blocked (i.e., frozen).[5]

RISKS

Continued use of products or services from a sanctioned entity, directly or indirectly through a service provider, may increase operational and OFAC compliance risk for a financial institution and could result in violations of law, civil money penalties, enforcement actions, and damage to the financial institution's reputation.

RISK MITIGATION

Financial institutions should ensure that their OFAC compliance and risk management processes address the challenges arising from possible interactions with a sanctioned entity. Identifying, assessing, and mitigating any risks associated with these sanctions requires a high degree of collaboration across a financial institution's OFAC compliance, fraud, security, IT, third-party risk management, and risk functions to assess any potential risk.

OFAC Compliance Program Risk Assessment

The Executive Order may increase OFAC sanctions compliance risk for some U.S. financial institutions. Financial institutions should assess their individual OFAC sanctions compliance risks and identify potentially impacted relationships and transactions. Additionally, financial institutions should ensure that their sanctions screening systems are updated and confirm that they have processes and procedures in place to comply with these sanctions.

Continued use of products and services from a sanctioned entity may cause the financial institution to violate OFAC sanctions. These sanctions prohibit U.S. persons — including U.S. financial institutions — from conducting transactions with sanctioned entities. Prohibited transactions include trade or financial transactions and other dealings, which may be broadly interpreted to include technical transactions such as downloading a software patch from a sanctioned entity.

Given the complexities of some of these third-party relationships and transactions relative to the sanctions, affected financial institutions are encouraged to contact OFAC, their legal counsel, and/or their security offices for additional guidance.

---

[3] https://home.treasury.gov/news/press-releases/sm0410

[4] Prohibited transactions are trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute. See OFAC's FAQ.

[5] Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property. See OFAC's FAQ.

Operational Risk Management

In addition to the violation of an OFAC sanction, continued use of software and technical services from a sanctioned entity may increase cybersecurity risk for a financial institution. Security software often operates within sensitive areas of an organization's infrastructure to identify vulnerabilities, ensure data is protected, or block malware. Because of the nature of the claims under OFAC's Cyber-Related Sanctions Program, a financial institution should assess the risk of having or continuing to use software and services from a sanctioned entity, and take appropriate corrective action.

Third-party service providers also may have used, or continue to use, products and services of a sanctioned entity on behalf of a financial institution. Accordingly, a financial institution should understand how its third-party service providers ensure compliance with the OFAC requirements.[6]

In some cases the sanctioned entity may be providing a critical service or control that cannot be discontinued instantly. If the products or services of a sanctioned entity provide a vital or necessary control, a financial institution should identify and implement an alternative solution at the earliest possible time. Financial institutions should contact OFAC for additional guidance as soon as possible if they encounter any operational issues related to sanctions deadlines. Financial institutions can reach OFAC through its telephone hotline at 1-800-540-6322 or by email at ofac_feedback@treasury.gov.

ADDITIONAL RESOURCES

The following government resources provide assistance to institutions for managing cyber-related sanctions risk.

OFAC Cyber-Related Sanctions Program
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

OFAC FAQs: General Questions
https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx

OFAC - Sanctions Programs and Information
https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

Sanctions Related to Significant Malicious Cyber-Enabled Activities
https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx

[6] https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_037.htm

FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet
https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

FFIEC Information Technology Examination Handbook, Information Security Booklet
https://ithandbook.ffiec.gov/it-booklets/information-security.aspx