Information Notice

Heightened Terror Threat Risk

January 23, 2020

Summary

The United States Department of Homeland Security (DHS) has issued a bulletin under the National Terrorism Advisory System summarizing the heightened risk of potential cyber and physical attacks by Iran against the United States.[1] This *Notice* outlines steps firms may consider taking to be prepared and respond to any cyber attacks and other business disruptions that may occur.

Background and Discussion

A January 18, 2020, National Terrorism Advisory System Bulletin issued by DHS outlines recent developments and trends regarding the potential terrorist threat that Iran may pose to the United States. While stating that there is no information indicating a specific, credible threat, the bulletin notes that Iran and its partners, such as Hizballah, have demonstrated the intent and capability to conduct operations within the United States, and that an attack may come with little or no warning. The bulletin states that Iran maintains a robust cyber program and is capable, at a minimum, of carrying out attacks that could temporarily disrupt critical U.S. infrastructure.[2] In addition, the bulletin notes the possibility of homegrown violent extremists sympathetic to Iran launching individual attacks.

In determining how to identify and respond to potential cyber and physical threats, member firms may consider taking the following actions:

- Adopt a state of heightened awareness and consistently review relevant threat intelligence and alerts.[3]
- Review the firm's cybersecurity program and procedures to determine if they would enable the firm to identify, prevent, and mitigate potential terror-related cyber threats.[4]
- Review the firm's business continuity and contingency plan (BCP) to determine if it would enable the firm to respond adequately to potential disruptions that may occur.[5]
- Increase organizational vigilance (*e.g.*, ensure appropriate personnel are monitoring key internal security capabilities, including proper system access, and understand how to identify anomalous behavior).[6]

Suggested Routing

- Compliance
- Legal
- Operations
- Registered Representatives
- Senior Management
- Systems
- Trading

Key Topic(s)

- Anti-Money Laundering
- Business Continuity Planning
- Cybersecurity
- Office of Foreign Assets Control
- Terrorist Activity
- Terrorist Financing

FINRA®

Endnotes

1. *See* National Terrorism Advisory System Bulletin, January 18, 2020 (replacing an expired January 4, 2020 bulletin). The bulletin expires on March 18, 2020.

2. *See* National Terrorism Advisory System Bulletin, *supra* n.1. *See also* Cybersecurity and Infrastructure Security Agency (CISA) National Cyber Awareness System Alert AA20-006A – Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad (January 6, 2020) (alert providing information to the cybersecurity community as a primer for assisting in protecting the United States' critical infrastructure in light of the current tensions between Iran and the United States and Iran's historic use of cyber offensive activities to retaliate against perceived harm).

3. *See, e.g.*, National Terrorism Advisory System Bulletin, *supra* n.1; CISA National Cyber Awareness System Alert AA20-006A, *supra* n.2. *See also* CISA INSIGHTS – Increased Geopolitical Tensions and Threats (January 6, 2020).

4. FINRA's cybersecurity web page provides useful guidance, such as FINRA's 2018 Report on Selected Cybersecurity Practices, FINRA's 2015 Report on Cybersecurity Practices and Core Cybersecurity Controls for Small Firms, on how to strengthen and develop cybersecurity programs.

5. *See* CISA INSIGHTS, *supra* n.3. In addition, firms can review the guidelines in the joint advisory issued by FINRA, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) providing best practices to the securities industry on business continuity and disaster recovery. *See Regulatory Notice 13-25* (FINRA, the SEC and CFTC Issue Joint Advisory on Business Continuity Planning) (August 2013).

6. *See* CISA National Cyber Awareness System Alert AA20-006A, *supra* n.2.