With a continued focus on Cybersecurity this month, firms should be aware of the United States Department of Homeland Security (DHS) bulletin issued 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.

HEIGHTENED TERROR THREAT RISK

BACKGROUND AND DISCUSSION

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]

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.

ATTENTION TO FIRMS WHO VOTE PROXIES

On August 21, 2019, the SEC issued guidance for firms who vote proxies on behalf of their clients (see SEC guidance). As a good measure – we recommend taking a look at your firm's Compliance Manual and the section specifically regarding Proxy Voting. A Firm's policies should explicitly state that the adviser votes proxies in the best interest of its clients. The policies also should address:

a. **Scope of Adviser's Voting Responsibility** – What parameters are used to serve the client's best interests; When the adviser will refrain from voting (e.g., too costly, or SEC lending restrictions);
b. **Explain Obligation to Multiple Clients** – Does the adviser vote all clients the same, and how is that in their best interest? How do you assess more complicated matters (e.g., M&A activity) that may require more analysis for each client;
c. **How the firm tests its compliance** (e.g., sampling as part of the annual review) and review the adequacy and implementation of your policies, which should be done and documented at least annually. (For example, if a firm employs a proxy voting service, the firm could compare the service's report to the information the firm obtains from the custodian as to which proxies the firm should have received and therefore voted.);
d. **Using Proxy Advisory Firms** – Adviser should assess the "capacity and competency" of the firms, including reviewing staffing, personnel, and technology. The firm also should, in the context of the services being provided,
    1. *Identify and evaluate* the proxy advisory firm's conflicts (this should be ongoing);
    2. *Ensure proxy service provides updates* regarding relevant business changes that may impact the provider's capacity and competency to provide services;
    3. *Conduct sampling and testing* the quality and accuracy of the proxy service recommendations;
    4. *Evaluate the service provider's sources* of information and methodology, including ensuring policies provide for consideration of additional information that may become available;
    5. *Evaluate those matters* where the proxy service's policies do not address how to vote on a particular matter (e.g., contested director election); and
    6. *Annually review* the adequacy of the proxy service policies.
    7. *Ensuring votes are not based on erroneous or incomplete information* and how to respond to errors.

CCO TIP:

- ✓ ***Enhance your policies and procedures*** to track what you are doing and to conform to the SEC guidance, and document your testing.
- ✓ **We should anticipate that all proxy voting services**, such as ISS & Broadridge, are going to prepare a **standardized report** that firms can request that addresses a number of the "capacity and competency" questions.