NEW YORK STATE OF OPPORTUNITY. Department of Financial Services

ANDREW M. CUOMO
Governor

LINDA A. LACEWELL
Superintendent

January 4, 2020

To: All Regulated Entities

Subject: Cybersecurity Risk Alert

There is currently a heightened risk of cyber attacks from hackers affiliated with the Iranian government.[1] The Iranian government has vowed to retaliate against the United States for the death of Qassem Soleimani. Given Iranian capabilities and history, U.S. entities should prepare for the possibility of cyber attacks.

It is particularly concerning that Iran has a history of launching cyber attacks against the U.S., and the financial services industry. For instance, in 2012 and 2013, Iranian-sponsored hackers launched denial of service attacks against several major U.S. banks. And the U.S. government recently advised in June 2019 it observed "a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies," and that Iranian attackers were increasingly using highly destructive attacks that delete or encrypt data.[2]

DFS therefore strongly recommends that all regulated entities heighten their vigilance against cyber attacks. While currently there are no specific, credible, reports of new Iranian-sponsored cyber attacks in the past few days, all regulated entities should be prepared to respond quickly to any suspected cyber incidents. Iranian-sponsored hackers have historically relied primarily on common hacking tactics such as email phishing, credential stuffing, password spraying, and targeting unpatched devices.

DFS therefore recommends that all regulated entities ensure that all vulnerabilities are patched/remediated (especially publicly disclosed vulnerabilities), ensure that employees are adequately trained to deal with phishing attacks, fully implement multi-factor authentication, review and update disaster recovery plans, and respond quickly to further alerts from the government or other reliable sources. It is particularly important to make sure that any alerts or incidents are responded to promptly even outside of regular business hours – Iranian hackers are

[1] There have been a number of media reports regarding the heightened risk. For example, see https://www.nytimes.com/2020/01/03/us/politics/homeland-security-iran-threat.html.

[2] See DHS, Cybersecurity and Infrastructure Security Agency, Statement on Iranian Cybersecurity Threats, June 19, 2019, at https://www.dhs.gov/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats. There have been media reports on the increasing risk of Iranian cyber attacks, such as https://www.forbes.com/sites/zakdoffman/2019/11/14/secret-iranian-network-behind-aggressive-us-cyberattacks-exposed-in-new-report/ - d3b7f5579cc8.

known to prefer attacking over the weekends and at night precisely because they know that weekday staff may not be available to respond immediately.

Regulated entities should also promptly notify DFS of any significant or noteworthy cyber attack. DFS's cyber regulation requires notification "as promptly as possible but in no event later than 72 hours" after a material cybersecurity event. 23 NYCRR 500.17. And, in light of the current threat, we urge all regulated entities to notify DFS of any material incidents as soon as possible given the heightened risk, and certainly no later than the required 72 hours. This will enable DFS to disseminate information about new cyber attacks as quickly as possible.

Any questions or comments regarding this alert should be directed to CyberAlert@dfs.ny.gov.

Sincerely,

Linda A. Lacewell
Superintendent

Justin S. Herring
Executive Deputy Superintendent, Cybersecurity Division