January 8, 2020

Valued CIRMA Members:

The Division of Emergency Management and Homeland Security (DEMHS) participated on a national conference call today with the Cybersecurity and Infrastructure Security Agency (CISA) regarding increased geopolitical threats pertaining to the increased tension with Iran.

In addition to the information contained herein, please visit CISA.gov for guidance on hometown security.

A National Terrorism Advisory Bulletin was released, Saturday January 4, 2020. This bulletin did not raise the alert level, however, did raise awareness.

On Monday, January 6, 2020, two products were released: (1) *CISA Insights on Threats. Simple Actions You Can Take,* and; (2) *CISA Cyber Activity Alert*—this product is more technical in nature and provides detailed information. Please heighten situational awareness regarding:

Cyber Risks:

1. Local Temporary disruptive/destructive effects
2. Increasingly sophisticated cyberattacks and espionage. Government, private sector, academic, think tanks wanting to know U.S. policies and thinking. **Note: Monitor INDUSTRIAL CONTROL SYSTEMS.**
3. Social media with anti-American, pro-Iranian messaging

Physical risks; particularly in the Middle East, including military installations—three types of actors have been identified:

1. Iran's Islamic Revolutionary Guard, Iranian actors and their intelligence services
2. Proxy Actors who take guidance from Iran but are not under its direct control
3. Proxy Actors that don't answer the call from the Iranian Supreme Leader but are radicalized

CISA recommends organizations take the following actions:

1. **Adopt a state of heightened awareness.** This includes minimizing coverage gaps in personnel availability, more consistently consuming relevant threat intelligence, and making sure emergency contact numbers are up to date.
2. **Increase organizational vigilance.** Ensure security personnel are monitoring key internal security capabilities and that they know how to identify anomalous behavior. Flag any known Iranian indicators of compromise and tactics, techniques, and procedures (TTPs) for immediate response.
3. **Confirm reporting processes.** Ensure personnel know how and when to report an incident. The well-being of an organization's workforce and cyber infrastructure depends on awareness of threat activity. Consider reporting incidents to CISA to help serve as part of CISA's early warning system.
4. **Exercise organizational incident response plans.** Ensure personnel are familiar with the key steps they need to take during an incident. Do they have the accesses they need? Do they know the processes? Are your various data sources logging as expected? Ensure personnel are positioned to act in a calm and unified manner.

> Click HERE to download the **CISA Insights – Increased Geopolitical Tensions and Threats** alert