April 24, 2020

Physical Security Considerations
for the
Healthcare Industry During COVID-19 Response

On March 24, 2020, law enforcement authorities attempted to make a probable-cause arrest in the Kansas City, MO area of a suspect who was planning to use a vehicle-borne improvised explosive device to cause severe harm and mass casualties at a local hospital. The event highlights potential threats posed to the healthcare system during COVID-19 response efforts, which could disrupt operations or harm healthcare personnel and those seeking medical assistance. Terrorists and other violent extremists may attempt to exploit the situation or vulnerable individuals may be triggered by stressors to commit disruptive or violent acts targeted at the healthcare community. This is particularly concerning as Healthcare and Public Health Sector continuity-of-operation is paramount to the national response to the pandemic.

As with any critical incident or threat involving healthcare facilities, the first call should be to local law enforcement agencies. In addition, the Cybersecurity and Infrastructure Security Agency (CISA), Health and Human Services (HHS), and the Federal Bureau of Investigation (FBI) also stand ready to support healthcare organizations to address security concerns. A wide range of resources are available to share threat and incident information, assist in decision-making, and enhance security capabilities.

The following provide web-based entry points for seeking security assistance and access to various resources:

DHS Cybersecurity and Infrastructure Security Agency (CISA)

- Coronavirus Webpage (https://www.cisa.gov/coronavirus): Provides information on COVID-19-related risks as well as tailored guidance for critical infrastructure providers and others on best practices, mitigations, and authoritative resources for additional information.
- Hometown Security Initiative (https://www.cisa.gov/hometown-security) and Office for Bombing Prevention (https://www.cisa.gov/office-bombing-prevention-obp): Provide access to training, tools, exercise, and other resources on a wide range of attack types (e.g., bombing, active shooter).

HHS Office of the Assistant Secretary for Preparedness and Response (ASPR)

- ASPR's Division of Critical Infrastructure Protection (CIP) coordinates with all levels of government and the private sector to assess cyber and physical threats and develop guidance to mitigate risks across the Sector to promote resilience. To obtain additional information, contact cip@hhs.gov.
- CIP provides regular threat and risk mitigation information through weekly Healthcare and Public Health newsletters. Sign up to receive the Cybersecurity or Preparedness, Resilience and Response bulletins here: (https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx).

DOJ Federal Bureau of Investigation (FBI)

- FBI Field Office and Joint Terrorism Task Forces (https://www.fbi.gov/contact-us/field-offices) carry out investigations, assess local and regional threats, and work closely with stakeholders on cases and operations.
- DHS-FBI *Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance* (SRG C-IED), (https://www.cisa.gov/publication/security-and-resiliency-guide-and-annexes), and its recently released annex for Healthcare and Public Health Facilities.