Update from the U.S. re: Coronavirus COVID-19

The U.S. Department of Homeland Security (DHS), the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Centers for Disease Control (CDC) recently held a joint call to address industry stakeholders regarding the current state of the coronavirus.

CISA has issued recommendations to industry with an aim to mitigate impact to business and enable operations to continue as much as possible. The recommendations from CISA are at the end of this email. CISA has a series of tools and resources that will be distributed in the coming days to facilitate with planning, including a Business Continuity Planning reference guide, a "Pandemic Guide", and brief resources to assist managers in working through challenges. Information and updates can be found on the CISA website.

In addition to CISA's documents, the following may also be useful:

- FEMA – Pandemic Influenza Template
    - This template provides guidance to assist organizations in developing a Pandemic Influenza Continuity of Operations Plan.

The CDC provided a short update on the virus. In the U.S. there are now 60 cases in 12 states. There are key identifiers for increased risk such as: those people in locations where there is community spread, health care workers treating patients with coronavirus, others in close contact with patients with coronavirus, and those traveling from or to international areas where the virus is known. At this time there is no vaccine. There are travel notices in effect for the following areas: China, Iran, South Korea, Italy, Japan and Hong Kong. CDC resources can be found at the following links:

- Checklist For Businesses
- Checklist For Businesses with Overseas Operations
- Site with pandemic resources

Lastly, DHS and CISA are working with the U.S. Department of Commerce, the White House and the National Economic Council to try and understand the disruptions to the supply chain. Companies experiencing issues are asked to get in touch with DHS at Sector.partnership@hq.dhs.gov. The agencies will collect this information and make any trending information publicly available. The agencies are also seeking feedback on "How is industry helping industry?" Companies are encouraged to ask vendors and partners what measures they are taking to help industry adapt to a shift towards telework and other measures.

Recommendations from U.S. Cybersecurity and Infrastructure Security Agency include the following:

1. If there is a plan to increase the number of workers that will “telework”, be mindful of the anticipated increase in “phishing” emails and cybersecurity threats. It is strongly recommended that companies review current cybersecurity prevention measures and ensure security is in place.
    a. Ensure VPN’s and remote access are tested
    b. Ensure required licenses are in place for teleworkers
    c. Enhance system monitoring
    d. Introduce two-step verification

2. Review and update preparedness plan or Business Continuity Plans (BCP) that may already be in place, or where there aren’t any, it is encouraged to implement a plan. CISA will issue some guidance around BCP’s shortly to assist with the process of developing and implementing a BCP.

3. Assign a point person to manage the Business Continuity Plan and oversee strategies to mitigate impact.

4. Ensure that essential goods, services and people are clearly defined as well as strategies for when these goods, services and people are not available. Is the business prepared for a personnel shortage?

5. Monitor and manage employee travel (whether business or pleasure) particularly where travel is to high risk areas.

The calls will be held regularly. Please monitor your inbox for updates and resources available to facilitate planning in response to the coronavirus and remember to wash your hands.