Overview

For additional guidance, please refer to Steptoe’s COVID-19 Resource Center.

On March 19, the Cybersecurity & Infrastructure Agency (CISA), which is part of the Department of Homeland Security, issued a memorandum providing guidance to help state and local jurisdictions, as well as private industry, with the “identification of essential critical infrastructure workers during COVID-19 response” (Guidance). CISA’s guidance can be found here.

CISA issued this Guidance after some local public health agencies had issued broad shelter-in-place (SIP) or stay-at-home orders that failed to define “essential” businesses or otherwise established narrow definitions. CISA explained that, consistent with its mandate to provide “strategic guidance” and “to promote a national unity of effort,” this Guidance is intended to assist state and local governments to identify sectors and functions that should be deemed “essential” and excluded from SIP or stay-at-home orders. Because state and local governments typically have responsibility for public health measures within their jurisdictions, the Guidance states that it is only “advisory” and not intended to be a federal directive. However, the Guidance is meant to represent an informed baseline for decision making, and certain states and localities are incorporating CISA’s guidance into COVID-19 related restrictions.

This client alert provides an overview of CISA’s Guidance.

Federal Government Guidance on Critical Infrastructure Workforce

The Guidance starts by emphasizing the importance of continuity for the nation’s critical infrastructure: “If you work in a critical infrastructure industry …, you have a special responsibility to maintain your normal work schedule.”[1] To identify individuals working in those industries, the Guidance appears to track most of the “critical infrastructure” sectors identified in Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience. This directive established 16 “critical infrastructure sectors, whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national economic security, national public health or safety, or any combination thereof.”

For COVID-19, CISA’s Guidance addresses the following critical infrastructure sectors:
 Within those sectors, the Guidance provides an "initial" list of the "Essential Critical Infrastructure Workforce," which it describes as the "workers who conduct a range of operations and services that are essential to continued critical infrastructure viability, including staffing operations centers, maintaining and repairing critical infrastructure, operating call centers, working construction, and performing management functions, among others."

According to CISA, the list can "inform critical infrastructure community decision-making to determine the sectors, subsectors, segments, or critical functions that should continue normal operations, appropriately modified to account for Center for Disease Control (CDC) workforce and customer protection guidance." This is an initial list because CISA expects that its list will evolve as it receives feedback on the listed sectors/subsectors and essential workers.

CISA's list includes the following examples:

**CRITICAL MANUFACTURING**
- Workers necessary for the manufacturing of materials and products needed for medical supply chains, transportation, energy, communications, food and agriculture, chemical manufacturing, nuclear facilities, the operation of dams, water and wastewater treatment, emergency services, and the defense industrial base.

**DEFENSE INDUSTRIAL BASE**
- Workers who support the essential services required to meet national security commitments to the federal government and US military. These individuals, include but are not limited to, aerospace; mechanical and software engineers, manufacturing/production workers; IT support; security staff; security personnel; intelligence support, aircraft and weapon system mechanics and maintainers.
- Personnel working for companies, and their subcontractors, who perform under contract to the Department of Defense providing materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities.

**FINANCIAL SERVICES**
- Workers who are needed to process and maintain systems for processing financial transactions and services.
- Workers who support financial operations, such as those staffing data and security operations centers.

**INFORMATION TECHNOLOGY**
- Data center operators, including system administrators, HVAC & electrical engineers, security personnel, IT managers, data transfer solutions engineers, software and hardware engineers, and database administrators.
- Workers supporting the provision of essential global, national and local infrastructure for computing services (incl. cloud computing services), business infrastructure, web-based services, and critical manufacturing.

**PUBLIC WORKS**
- Workers who support the operation, inspection, and maintenance of essential dams, locks and levees, essential public works facilities and operations, including bridges, water and sewer main breaks, fleet maintenance personnel, construction of critical or strategic infrastructure, traffic signal maintenance, emergency location services for buried utilities, maintenance of digital systems infrastructure supporting public works operations and other emergent issues.

Recognizing a need for certain deference to state/local authorities, the Guidance includes caveats. It states, for example, that "this list is advisory in nature;" that "it is not, nor should it be considered to be, a federal directive or standard in and of itself;" and that "state and local officials should use their own judgment in using their authorities and issuing implementation directives and guidance."
Defense Industrial Base

Certain federal agencies have issued additional guidance on the critical infrastructure workforce. On March 20, 2020, the US Department of Defense (DoD) issued two memoranda regarding the Defense Industrial Base Essential Critical Infrastructure Workforce.[2] For this critical infrastructure sector, DoD explains:

Companies aligned with the essential critical infrastructure workforce definition are expected to maintain staffing and work schedules necessary to meet contract requirements. In some cases, this may be the normal work schedules that had been in place before the declared national emergency.[3]

DoD also said the defense-related essential workforce includes (1) contractor personnel performing under orders rated by DoD under the Defense Priorities & Allocation System and (2) those performing under unrated orders that directly support mission readiness and national security.

Different Approaches for State-Wide Orders

On March 19, 2020, the Governors of California and Pennsylvania issued statewide SIP orders, with each state taking a different approach to identifying exceptions to their orders.[4] California's order followed CISA’s Guidance and excluded “Essential Critical Infrastructure Workforce” from the order, stating that its order did not apply to those workers “needed to maintain continuity of operations of the federal critical infrastructure sectors.”[5]

Pennsylvania, on the other hand, issued a state-wide ban on most business activities, except “life-sustaining” ones. As initially issued, Pennsylvania's ban did not expressly reference or refer to CISA’s “Essential Critical Infrastructure Workforce.” On Saturday evening (March 21), however, Pennsylvania had revised the list to include some references to CISA’s Guidance, stating, for example, that “defense industrial base manufacturing under CISA is permitted” and “financial services under CISA is permitted.”[6]

Although CISA’s Guidance should help state/local jurisdictions and private industry identify the essential workforce needed to perform despite efforts to mitigate the impact of COVID-19, private industry also must consider specific orders and guidelines issued by state and local governments — many of which continue to revise and update their directions. It also will be important for private industry to communicate with state and local officials as well as federal representatives and regulatory agencies regarding the impact of local SIP and stay-at-home orders on critical operations. Businesses also should consider other necessary external and internal communications for suppliers and employees regarding determinations to continue operations considered to be “essential.” Steptoe is working with many clients to navigate these issues in order to ensure the continuity of the nation’s critical infrastructure.

[2] See March 20, 2020 Memo from DoD’s Under Secretary of Defense for Acquisition and Sustainment (A&S); March 20, 2020 Memo from DoD’s Office of the Under Secretary of Defense for Defense Pricing and Contracting. Other federal agencies are beginning to issue similar letters, and more should be expected.
[4] Other states are taking similarly diverse approaches, and some are modifying their orders to accommodate more of the Guidance.
[6] Pennsylvania’s revised list of “life-sustaining” businesses is linked here.

Practices
Privacy & Cybersecurity
Government Contracts
Labor & Employment
Chemicals & Environment

© 2020 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.