

Think Twice About Claiming Essential Critical Industry Status

Related Professionals

Sarah Sloan Batson
864.282.1113
SBatson@nexsenpruet.com

David J. Garrett
919.653.7802
dgarrett@nexsenpruet.com

David S. Robinson
919.653.7809
DRobinson@nexsenpruet.com

Mark Bakker
864.282.1175
MBakker@nexsenpruet.com

Practices

Employment & Labor Law

03.25.2020

Before your company determines it is in an Essential Critical Industry (ECI), think twice. There are already reports of some employers who are abusing the hastily-written descriptions of ECI, falsely claiming to be an ECI when in fact they are not. A false claim to being an ECI not only exposes the company's workers but also their workers' families (who certainly have at risk people in their households) to risks of contagion that may later be found to be unreasonable risks. While intentions are noble to maintain jobs and the investments of stakeholders, such a decision can have significant consequences. In addition to fines or penalties for violations of such orders, civil liability is another significant concern.

Risks Associated with an Incorrect ECI Determination

The immediate risk to any company that continues operations, of course, is the loss of a worker who becomes ill and the quick spread of the virus throughout your workforce, leaving you with an uptick of sudden sick leave. But what happens later?

All companies have a duty to protect their workers, and companies who falsely claim to be ECI may later be found to be negligent – and perhaps grossly negligent. Requiring nonessential employees to report to the workplace or violating a stay at home order and thereby exposing employees to the virus can lead to allegations of negligence and negligent supervision. If customers or end users in receipt of products handled by a company's infected employees believe they have been unnecessarily exposed, this could also lead to potential claims of negligence. Most insurance policies specifically disclaim coverage for intentional torts, as well as for contagious diseases. In these situations, if decisions are viewed as reckless or negligent, personal liability to certain managers is a potential risk.

In addition, the company risks severe reputational exposure. In today's culture, many workers are adept at calling out unscrupulous company actions. Companies do not want to face a public relations disaster, or be accused of being reckless and unpatriotic by unnecessarily exposing

workers in this particular emergency.

As many states are implementing and enforcing Stay at Home orders, many employers are scrambling to find ways to ensure continuity in their business to keep their employees working, servicing their customers, and ultimately save profits. Some employers are finding gray area in these orders and managing to self-certifying their business as being exempt from Stay at Home orders, reasoning that the company is an Essential Critical Infrastructure provider. It is important for businesses to consider the short and long-term risks in making this determination, as exposure following the pandemic for a knowingly false ECI designation could be far greater than the present financial crisis imposed by compliance.

What is an ECI provider?

The broad definition of critical infrastructure is defined in the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)). ‘Critical infrastructure are any “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” This definition is appropriately broad to include a wide range of stakeholders who either directly or indirectly enable the functionality of infrastructure systems.’

During the COVID-19 pandemic, the Federal Cybersecurity & Infrastructure Security Agency (CISA) is responsible for defining our critical infrastructure and for protecting this infrastructure from physical and cyber threats. Functioning critical infrastructure is imperative during the response to the COVID-19 emergency for both public health and safety as well as community well-being. Certain critical infrastructure industries have a special responsibility in these times to continue operations. CISA guidance is intended to support state, local, and industry partners in identifying the critical infrastructure sectors and the essential workers needed to maintain the services and functions Americans depend on daily and need to be able to operate resiliently during the COVID-19 pandemic response. This document gives guidance in defining essential critical infrastructure workers. Promoting the ability of such workers to continue to work during periods of community restriction, access management, social distancing, or closure orders/directives is crucial to community resilience and continuity of essential functions.

CISA guidance lists 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 security, national economic security, national public health or safety, or any combination thereof:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector

- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

It is important to note that although the vast majority of stay at home declarations are based on the CISA categories, many state and local governments have expanded upon, or attempted to clarify, this federal guidance. Ultimately, it is up to state and local governments to enforce Stay at Home orders, and it is the state and local governments' definitions and interpretations of CISA that will apply to your company.

Making and Documenting the ECI Determination

Given that businesses are largely forced to self-document at this time, we strongly recommend that companies create substantive contemporaneous documentation supporting their determination.

Good documentation demonstrates a reasonable method, reasonably applied. The record should accurately and completely describe the analyses conducted by the business, and the resulting determinations. This documentation could include the following 10 items:

1. Overview of the business
2. Description of the organizational structure of all business lines and organizational entities
3. Documentation regarding any and all applicable disaster declarations and warnings, including the above CISA guidance, as applicable
4. Analyses of business functions, operations, and occupations
5. Description of determinations made on a company-wide basis
6. Description of determinations made on a position basis, as applicable
7. Exceptions to any general rules for individuals or occupations
8. Notices to employees regarding determinations
9. Notices to particular employees when given any choices, with counter-signature requirements

10. Descriptions of why certain options discussed were not accepted/implemented

In making the analysis above, companies should keep in mind that the determination involves two important subparts: (1) Is the business (in full or in part) an ECI provider? (2) Which employees/positions are needed to physically report to the workplace to operate the business functions that are considered Essential Critical Infrastructure?

Even for non-essential business, depending on the applicable order and jurisdiction, there may be permitted activities by certain essential personnel that are needed to continue operations by employees or contractors who are working from home, such as IT, payroll, or other key functions. Documenting this analysis and equipping those employees with a letter certifying their justification for working and traveling outside of the home is important.

Practical Steps to Reduce Exposure and Maintain Operations

Finally, below are some practical tips to reduce exposure and maintain your business operations during this pandemic.

1. **Take every precaution to protect workers who continue to physically report to work in the workplace.** You should have guidance or protocols that employees are required to follow to protect themselves and their coworkers. This includes requiring ill or exposed employees to stay home, sanitizing the workspace, providing sanitizing wipes, personal protective equipment, and thoughtfully arranging work spaces, reducing in-person meetings, and limiting contact with customers, delivery workers, or even other coworkers unnecessarily.
1. **Permit employees to work from home when possible.** Under these unique circumstances, encourage employees who are able to work remotely from home, and be sure to document in writing your communication to employees, that their choice to work in the workplace is voluntary. This writing may later be an important defense to a future negligence claim. Importantly, consider refraining from employee discipline for attendance and offering leaves of absences (unpaid or using accrued and unused paid leave) to nonessential employees uncomfortable reporting to work given these circumstances.
1. **Plan for workplace exposure.** Have a plan in place to communicate with employees who may be exposed to COVID-19 in the workplace, to sanitize the workplace, and relocate employees working in that area until it is properly sanitized.
1. **Develop and implement a daily screening program for all staff.** For example, some health directives/departments are requiring employers implement the following precautions for companies that remain in operation:
 1. Screening criteria must include the following questions:
 1. Symptom check (fever, cough, shortness of breath, sore throat, diarrhea). When a touchless thermometer is available, a temperature check is strongly recommended in lieu of verbal confirmation.
 2. Any close contact in the last 14 days with someone with a diagnosis of COVID-19.
 3. Travel internationally or domestically in the last 14 days
 2. A yes to any of the screening questions above requires the employee to be excluded:

1. 3 days with no fever and 7 days since first symptom
 2. 14 days if close contact of diagnosed case of COVID-19
 3. 14 days following travel
1. Develop and implement a plan to manage and control social/physical distancing (at least 6 ft spacing) for employees working alongside one another and customers waiting in lines within or outside the business.
 1. Limit capacity inside facilities to provide for social distancing of customers and between customers and employees including but not limited to visual markings and signage; entrance limits and specialized hours.
 1. Publish this social distancing order at entrance of the facility and to the members of the public at large by all reasonable means available.

Most importantly, be proactive and thoughtful as you make decisions each day in balancing continued operations, worker safety, and social responsibility.

Our Insights are published as a service to clients and friends. They are intended to be informational and do not constitute legal advice regarding any specific situation.
