News You Can Use

June 2024
Volume 12
Issue 6

HEFFERNAN INSURANCE BROKERS

Because You're Different

Workplace Safety

Indoor Heat Illness Rules Coming Soon

THE CAL/OSHA Standards Board has voted to approve new heat illness prevention regulations that will require some workplaces to make significant adjustments to their operations in order to comply, possibly starting early this summer.

The vote has been challenged, and at the last minute the California Department of Finance withdrew its approval of the regulatory changes due to a lack of full analysis on their potential financial impact on state entities, particularly state-operated correctional facilities.

However, Cal/OSHA is already in the process of creating a carveout for these entities to appease the Finance Department.

The indoor heat illness prevention standard applies to most indoor workplaces where the temperatures reach at least 82 degrees. According to Cal/OSHA, that includes facilites like warehouses, manufacturing and production facilities, greenhouses, wholesale and retail distribution centers, restaurant kitchens and dry cleaners.

The rules

Applicable employers will need to create and maintain a written indoor heat illness prevention plan that includes the following:

82-degree trigger – When temperatures indoors reach this level, employers must:

- Have and maintain one or more cool-down areas when employees are present, which must be kept at a temperature below 82 degrees.
- Allow and encourage staff to take preventive cool-down rests in a cool-down area when they feel the need. They should be monitored for signs of heat illness during rests.
- Provide drinking water near the areas employees are working.
- Observe all employees during heat waves when a workplace has no measures for controlling the effects of outdoor heat on indoor temperatures.

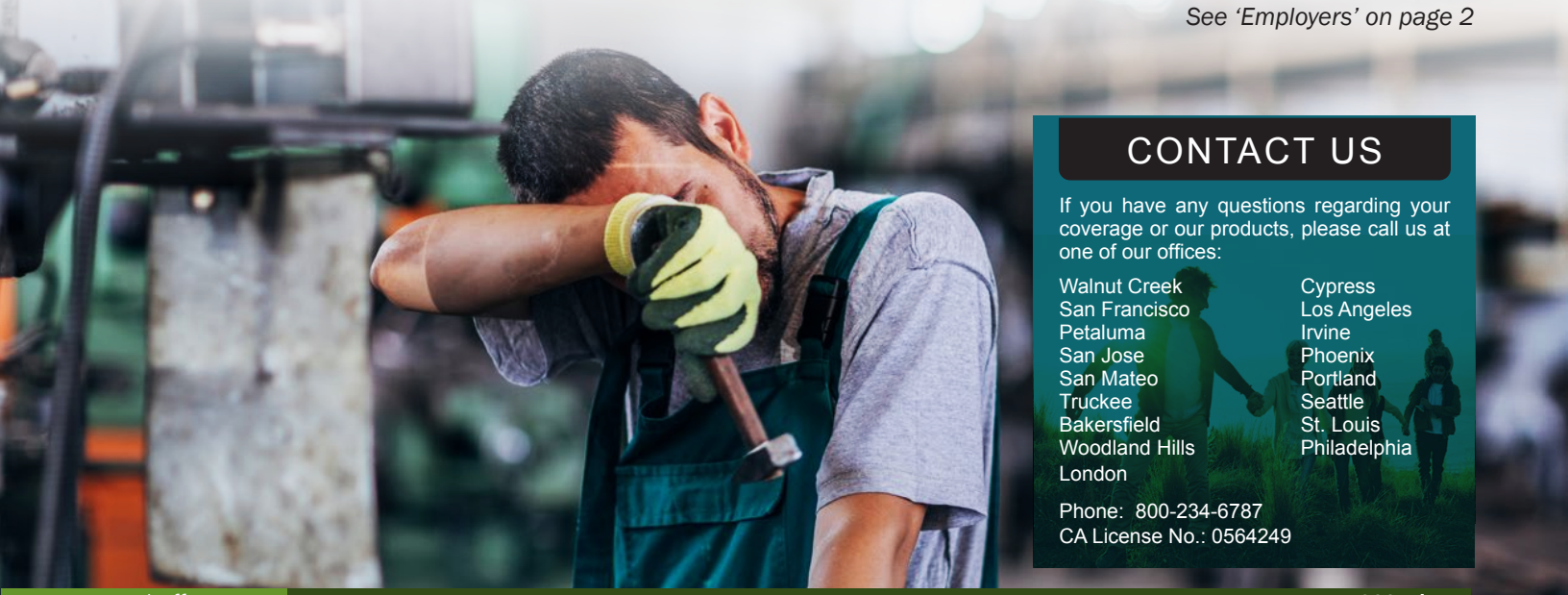
87-degree trigger – When the temperature exceeds 87 degrees, employers must measure the temperature and heat index, and identify all other environmental risk factors for heat illness. Firms must keep records of the temperature/heat index.

They must also implement control measures such as:

- Using air conditioners, swamp coolers, ventilation or other measures to reduce the air temperature (engineering controls);
- Adjusting work procedures, practices or schedules to minimize exposure to heat, such as changing shifts to start earlier and avoid the hottest parts of the day (administrative controls); or
- Using personal heat-protective equipment, such as water- or air-cooled garments or heat-reflective clothing.

Employers with affected workplaces must also observe new employees for 14 days when working under these conditions.

See 'Employers' on page 2



CONTACT US

If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek
San Francisco
Petaluma
San Jose
San Mateo
Truckee
Bakersfield
Woodland Hills
London
Cypress
Los Angeles
Irvine
Phoenix
Portland
Seattle
St. Louis
Philadelphia

Phone: 800-234-6787
CA License No.: 0564249

Fed-OSHA Rulemaking

New Rule Lets Non-Employees Join Inspections

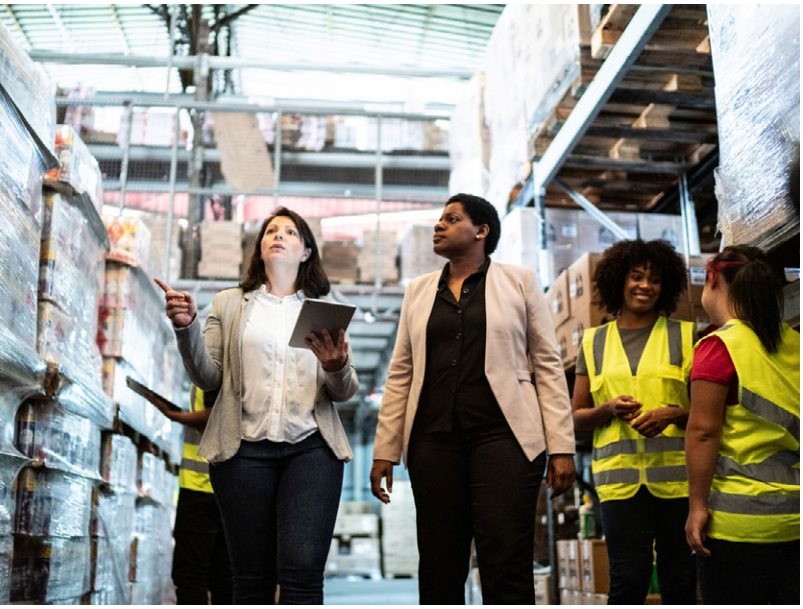
A NEW DEPARTMENT of Labor rule change clarifies the rights of employees to appoint an outside representative to accompany OSHA officers during workplace inspections.

OSHA inspections usually occur after a workplace has had a safety-related incident or a whistleblower has reported suspected safety violations. Attorneys representing employers say the new rule, which took effect May 31, could be problematic for businesses trying to keep inspections free of disruptions.

Advocates for employers worry that external observers may use their new ability to collect information that can be used to convince employees to join a union.

They also see a potential for other adversaries to join the inspections in search of employer failures. These might include disgruntled former employees, plaintiffs' attorneys, potential expert witnesses or injured workers' family members.

OSHA stressed that the final decision as to whether to permit a third party representative to join the inspection is up to the OSHA compliance safety and health officer that conducts the inspection. Either the employer or workers may appeal to the CSHO to reject a representative, but the CSHO decides.



In its response to public comments, OSHA emphasized the importance of employee representation to gathering necessary information about worksite conditions and hazards.

It also noted that the rule does not limit third party representatives to union representatives; third parties' ability to participate will be based on their knowledge, skills or experience.

"Third party representatives' sole purpose onsite is to aid OSHA's inspection," it wrote, "and CSHOs have authority to deny the right of accompaniment to third parties who do not do that or who interfere with a fair and orderly inspection."

Supporters of the rule argued that third parties may:

- Have important technical or subject matter expertise.
- Have language skills and cultural knowledge.
- Increase employees' trust in the inspections.
- Improve inspections of multi-employer worksites, such as construction sites.
- Balance the rights of employers and employees.

The takeaway

Employers may be more likely to face litigation and a difficult discovery process after an accident under the new rule, legal pundits say.

Some observers recommend that employers stand ready to object to participation from plaintiffs' attorneys who may not have much workplace safety expertise but who know how to fish for clients.

It will be important that they evaluate the need for a particular third party to participate in the inspection.

Employer groups are expected to challenge the new rule in court. A court might issue an injunction preventing the rule's enforcement during litigation.

That is uncertain, however, so employers should be prepared now to permit third parties to join OSHA inspectors on their premises if workers request it. ❖

Continued from page 1

Employers Must Develop Emergency Response Procedures

Emergency response – Employers must develop emergency response procedures, which must include:

- An effective communication system to allow workers to contact a supervisor or emergency services.
- Steps for responding to signs and symptoms of heat illness, including first aid and providing emergency medical services.
- Emergency response procedures for severe heat illness.
- Monitoring employees exhibiting signs of heat illness, and not leaving them alone without offering them on-site first aid or medical services.

Training – Employees and supervisors will need to be trained on:

- Personal risk factors for heat illness.
- Their employer's procedures for complying with the regulations.
- The importance of frequent water consumption.

The takeaway

As mentioned, at this point there is no definitive date for these regulations taking effect, but Cal/OSHA insists they will be ready before summer starts in late June. ❖

New Rulemaking

EEOC Issues Updated Workplace Harassment Guidance

THE EQUAL Employment Opportunity Commission has issued updated workplace harassment guidance for employers, increasing possible exposure to employee-initiated lawsuits.

These are federal guidelines, meaning that they open a new avenue for potential employment practices liability exposure. Employers should understand this new guidance to ensure they don't run afoul of the law and risk being sued by a worker.

The guidance includes the following:

Sex-based harassment

The guidance expands the definition of sex-based harassment to include harassment related to breastfeeding, morning sickness, contraception and decisions to obtain — or not obtain — an abortion.

It also expands protections to include harassment based on sexual orientation and gender identity.

An example of the latter would be an employer intentionally and repeatedly using a name or pronoun that is inconsistent with the worker's gender identity, or denying access to bathrooms that are consistent with their identity.

Virtual harassment

The guidance states that harassment can occur in the "virtual work environment," such as through the firm's e-mail system, electronic bulletin boards, instant message systems, videoconferencing technology, intranet or official social media accounts.

The EEOC stated that while off-duty offensive social media posts sent on work systems generally don't constitute harassment, they may if they impact the workplace, such as if the postings are directed at a particular employee or employer and are referenced at work.

The agency also stated that even if offensive material is sent while off-duty on non-work systems, like using personal phones or tablets to text harassing messages or making derogatory posts on their own social media accounts, it could be considered illegal.

The takeaway

The EEOC has designated workplace harassment as an enforcement priority.

You should update your anti-harassment policies and procedures in your employee handbooks to reflect the changes to EEOC guidance. Managers and supervisors should be trained in the new guidance as well. ❖

Policies the EEOC Recommends

- Define what conduct is prohibited.
- Be comprehensible to workers, including those whom you have reason to believe might have barriers to comprehension, such as limited literacy skills or proficiency in English.
- Require supervisors to report harassment incidents.
- Offer multiple ways to report harassment.
- Identify points of contact to whom reports of harassment should be made, including contact information.
- Explain your firm's complaint process, including the anti-retaliation and confidentiality protections.

VIRTUAL ICK: *Online harassment may constitute workplace harassment under EEOC's new guidance.*

Cyberattack Study

Business E-Mail Compromise Scams Top Threat

BUSINESS E-MAIL compromise scams are now the most common type of cyberattack businesses face, and all types of these attacks are showing no signs of letting up, according to a new report.

Nearly three out of every four businesses were targets of these attacks and 29% of those firms became victims of successful attacks, according to the report by Arctic Wolf, a cyber-security firm..

While this has become the most common type of attack, a number of other schemes like ransomware attacks and data breaches continue growing in number.

Any of these attacks can drain a company's finances and result in tricky legal and possibly reputational issues that take time and money time to resolve.

The trends

The main threats businesses face, according to the report, are:

Business e-mail compromise (BEC) – Seven in 10 organizations surveyed said they had been targeted by these types of scams.

Some examples of BEC attacks include impersonating company executives to request wire transfers, falsifying invoice payment details, and tricking employees into revealing sensitive information. These scams can result in significant financial losses for businesses.

CAUTION: For businesses that use cloud-based e-mail services like Office365, these attacks are hard to detect since they don't reside on company servers.

With many organizations moving to cloud-based e-mail services, these types of attacks can be difficult to identify with traditional security tools and may go undetected until they have successfully executed their objectives.

Data breaches – Nearly half (48%) of organizations surveyed reported that they'd found evidence of a breach in their systems. The authors said that does not mean that the other 52% didn't suffer a breach; it means they failed to find evidence of one.

Ransomware – Some 45% of organizations surveyed admitted to being the victim of a ransomware attack within the last 12 months. These attacks usually involve criminals gaining access to a company's systems by getting an employee to click on a malicious link, after which they lock down the system and demand a ransom to unlock it.

Increasingly, perpetrators are also stealing data and demanding a second ransom to give it back and not release the data to others.

What you can do

How to Protect Against BECs

- Register all domain names that are similar to the business's legitimate website and can be used for spoofing attacks.
- Create rules that flag e-mails received from unknown domains.
- Monitor and/or restrict the creation of new e-mail rules on your servers.
- Enable multi-factor authentication.
- Conduct BEC drills, similar to anti-phishing exercises.
- Companies that use Office 365 or other cloud-based e-mail services, should employ detection tools or services specifically designed to monitor for threats related to BEC scams.

To combat ransomware:

Regularly back up system. Verify your backups regularly. This way you can restore functions if hit by ransomware.

Store backups separately. In particular, store backups on a separate device that cannot be accessed from a network, such as on an external hard drive.

Training your staff. Train your staff in how to spot possible phishing e-mails that are designed to convince an employee to click on a malicious link that will release the ransomware. ❖