IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

SECURITY CONSIDERATIONS FOR COVID-19 VACCINE DISTRIBUTION

DEFEND TODAY, SECURE TOMORROW

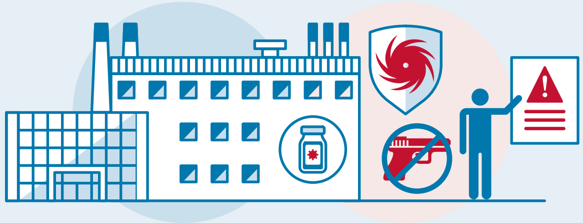
Sites producing or distributing the COVID-19 vaccine can take steps to enhance safety for their personnel. Although a physical attack is unlikely, individuals working in manufacturing and distribution sites, as well as vaccine recipients, may be vulnerable to various threats, including physical and cyber. Facility managers and operators should prepare Emergency Response Plans, enhance physical security, and implement processes and systems to bolster cybersecurity. Stakeholders can access information and updates related to critical infrastructure and the COVID-19 pandemic from the Cybersecurity and Infrastructure Security Agency (CISA) on CISA's Coronavirus Webpage (cisa.gov/coronavirus).

ABOUT THIS GUIDE

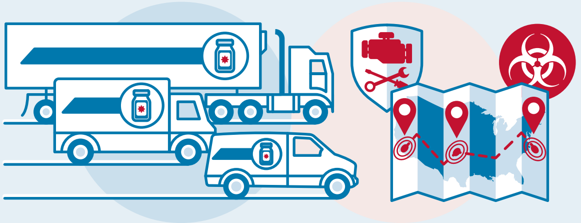
This guide provides information about potential physical threats to people and cyber threats to operations as the COVID-19 vaccine moves into wide distribution. It also suggests mitigations and directs readers to additional resources for further information to help protect life and property.

DISTRIBUTION STAGES

COVID-19 vaccines distribution broadly occurs in four stages: manufacturing centers, transportation units, traditional clinics, and points of distribution (PODs). Traditional clinics are places like pharmacies, nursing homes, and medical facilities, while PODs are satellite clinics established in areas like community centers, parking lots (outdoor), or public venues (indoor).

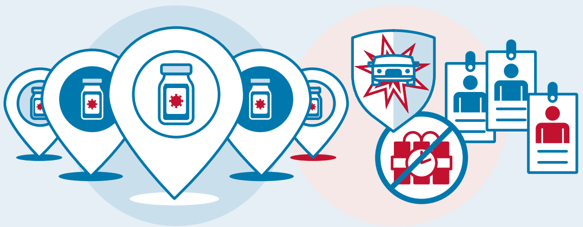


1 Manufacturing Sites



2 Transporters

3 Traditional Clinics



4 PODs

SATELLITE CLINICS AND VACCINE MOBILE UNITS

Vaccine distribution clinics may exist as mass vaccination sites in places like stadium parking lots, or smaller PODs in sites such as commuter stations, or even mobile units. PODs are subject to physical and cyber threats, many of which are addressed below.

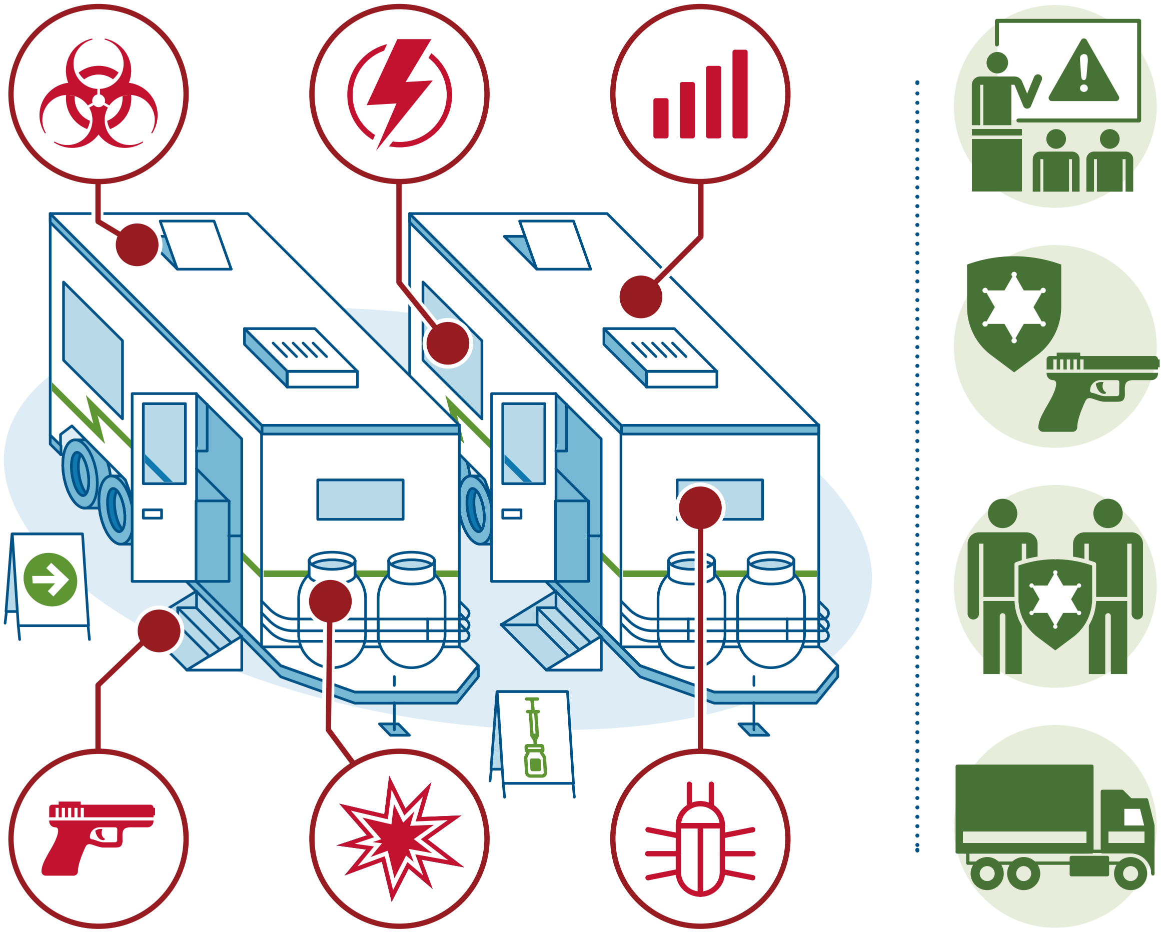
Vaccine mobile units can distribute vaccinations to populations that lack easily accessible pharmacies and hospitals, including rural communities and sites where workers are unable to step away from their manufacturing jobs.

Due to their transient nature, **vaccine mobile units may be especially vulnerable to physical and cyber threats**. To the extent possible, identify vulnerability gaps, and ensure robust cybersecurity measures on all onsite systems.

Due to a lack of space, mobile units are **unlikely to have permanent perimeter security or traffic control items** like ramps and fencing.

To help protect both PODs and vaccine mobile units, **educate volunteers, particularly screeners, on suspicious indicators** in people and vehicles.

Maintain armed security as a visible deterrent during set up, site operations, and after vaccination distribution efforts.



The **mobile units typically comprise two trailer-based operations**, occupying approximately 3,500 square feet. They set up in facility parking lots and contain equipment and several thousand vaccine doses.

Staff and **one or two dedicated law enforcement officials may be assigned to provide perimeter security** during mobile unit operations. Private security officers may provide security in some areas where law enforcement officers are limited or unavailable.

Vaccine mobile unit organizers should **ensure coordination with local government** to use available infrastructure, such as heavy vehicles, to create perimeter security where possible around the mobile units.

For More Information: Visit cisa.gov/publication/cybersecurity-and-physical-security-convergence and cisa.gov/publication/covid-19-vaccine-physical-security.

THREATS

Active Shooter

Active shooters, though unlikely, are possible at manufacturing sites, traditional clinics, and PODs. Temporary sites may be particularly vulnerable due to their ease of access. The Department of Homeland Security's (DHS) Run, Hide, Fight recommended approach provides actionable guidance for safety. In short, the guidance advises the following:

- Decide firmly and quickly on your actions.
- Commit to your choices, always attempting to escape the facility, if possible.
- When law enforcement arrives on the scene, quickly provide any information on the assailant, such as a physical description or their location.

To reduce the risk or scope of an active shooter, train employees to identify and report suspicious behavior in visitors and co-workers. DHS's If You See Something, Say Something® campaign teaches how to recognize and report suspicious activity. **Some suspicious indicators include:**

- Loitering in an unauthorized area, especially with no reasonable explanation
- Loitering, parking, or standing in the same area over multiple days with no reasonable explanation
- Attempting to gain information about the operations or security of facilities
- Displaying aggressive or erratic behavior that a reasonable person might find threatening
- Filming or surveilling workers and individuals beyond casual interest

Facility owners and managers should control access to facilities. Allow only credentialed workers to access restricted areas, and verify that all unknown individuals have a reasonable need to be present on facility grounds. Establish a facility-wide notification system so that staff and vaccine recipients are immediately notified of an emergency.

ℹ **For More Information:** Visit cisa.gov/active-shooter-preparedness; dhs.gov/see-something-say-something; cisa.gov/publication/insider-threat-mitigation-resources; and cisa.gov/employee-vigilance-power-hello.

Improvised Explosive Devices (IED) and Improvised Incendiary Devices (IID)

To eliminate areas for potential IED attack, remove trash bins that are accessible to the public onsite. Additionally, conduct periodic visual security sweeps of the operation to ensure no unattended backpacks or bags. In the event of a bomb or arson threat, immediately evacuate the area, and contact law enforcement and emergency responders. Meet at a known rally point after evacuating facilities to account for all personnel. Maintain situational awareness as first responders arrive.

To further mitigate the risk and scope of both IED and IID threats:

- Develop, update, and exercise Bomb Threat Management Plans.
- Train staff to recognize and report suspicious behavior and items, as well as evacuation of workers and guests.
- Ensure that emergency exit points are clearly marked.
- Restrict any areas within the facility that contain combustible materials to everyone except those with credentials and a reasonable need.
- Inspect vehicles for irregularities or damage before they leave facilities.

ℹ **For More Information:** Visit cisa.gov/office-bombing-prevention-obp and cisa.gov/publication/active-assailant-security-resources, where a guide to fire used as a weapon resides.

Vehicular Attack

A vehicular attack could occur as a vehicle-borne improvised explosive device (VBIED) or ramming.

These attacks could also be part of a complex coordinated attack (CCA), in which multiple assailants, weapons, and locations are involved. In the event of a vehicle ramming or CCA, DHS's Run, Hide, Fight methodology again provides an effective response protocol. If a suspected vehicle is reported, evacuate the area and notify first responders immediately.

PODs, especially vaccine mobile units, and transporters, may be the most vulnerable parts of the vaccine distribution chain to vehicular assaults due to their lack of existing physical security infrastructure. Where long car or pedestrian lines develop, traditional clinics may also become exposed to vehicular assault.

To mitigate the risk and scope of a vehicular attack:

- Prohibit pedestrian access to roads by erecting vehicular barriers.
- Plan vehicle ingress so that lanes follow a serpentine pattern and are a safe distance away from pedestrians.
- Set parking areas away from pedestrians entering PODs.
- Establish clear standoff zones, ensuring a solid passive barrier exists between workers on foot and vehicle lines.
- Ensure that drivers display valid credentials before granting delivery vehicles access to restricted areas.
- Immediately report any suspicious driver behavior and seemingly abandoned vehicles.

For More Information: Visit cisa.gov/securing-public-gatherings to view the Vehicle Ramming Guide; cisa.gov/publication/dams-vehicle-barriers-guide for guidance on selecting barriers at various facilities; youtube.com/watch?v=Yw-fY86WhRg for a video on vehicle-ramming mitigation; and the Joint Counterterrorism Assessment Team product, Vehicle-Borne Improvised Explosive Devices (VBIED): Preparedness, Recognition, and Response First Responder's Toolbox at dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox to view comprehensive information on VBIEDs.

Hijacking & Theft

Before vaccine deliveries begin, transport managers should ensure drivers are trained how to identify and report suspicious behavior during transit and at rest stops.

- While en route, drivers should not deviate from designated routes without clearance or make unapproved stops.
- To provide support to drivers and limit the opportunity for malicious actors to target transporters, provide vehicles with visible, armed security personnel.

For More Information: Visit tsa.gov/for-industry/firstobserver, tsa.gov/for-industry/resources, and phmsa.dot.gov/hazmat/erg/emergency-response-guidebook-erg.

Theft and counterfeiting are significant risks. To offset vulnerability to theft, regard COVID-19 vaccines as valuable cargo. Organized crime and other illegal sellers may attempt to steal doses for profit. Train staff to identify and report suspicious behavior, and ensure facilities maintain strict access controls for vaccine storage and dispensing. Access control can include the implementation of a dual employee authentication system. Dispose of empty vaccination containers according to established protocols to reduce the opportunity for criminals to create counterfeit vaccines. Within facilities, implement alarm systems, and ensure that Closed-Circuit Television (CCTV) systems are properly positioned to actively monitor vaccine storage areas.

For More Information: Visit dhs.gov/see-something-say-something/recognize-the-signs and dhs.gov/nsi.

Small Unmanned Aircraft Systems (sUAS)

Although beneficial for many survey and monitoring tasks, small unmanned aircraft systems (sUAS) can be used for malicious aims.

Bad actors can use sUAS to:

- ✓ Cause physical harm with onboard items like explosives or chemical agents
- ✓ Surveil existing security systems before committing an attack
- ✓ Commit cybercrimes like theft of intellectual property and generally disrupt systems

To mitigate risks posed by sUAS:

- ✓ Establish reporting pathways with law enforcement.
- ✓ Post No Drone signage to deter unwanted sUAS activity.
- ✓ Work with legal authorities before implementing any type of approved technology, such as jamming, spoofing, and hacking, to interfere with illegal sUAS capabilities.

For More Information: Visit cisa.gov/publication/uas-fact-sheets; cisa.gov/publication/uas-ci-drone-pocket-card; cisa.gov/publication/advisory-application-federal-laws-acquisition-and-use-technology-detect-and-mitigate; and cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems.

MISINFORMATION, DISINFORMATION, AND ANTI-VACCINATION PROTESTS

Given security incidents at COVID-19 testing and treatment sites in 2020 and vaccination sites in 2021, vaccine distribution sites organizers and managers should remain aware of potential disruption and threat by anti-vaccination protest groups. As misinformation on COVID-19 and the vaccine fuels online conspiracy theories, groups have formed with the intention of hindering the vaccine's distribution. Additionally, disinformation campaigns orchestrated by nation-state actors and domestic conspiracy theory purveyors will likely continue to try to dissuade Americans from seeking the vaccine.

To mitigate disruption:

- Ensure armed security staff are present during operation hours.
- Maintain awareness of potential nearby protest activities.
- Be prepared to pivot to alternative operation procedures or evacuation protocols.

CYBERSECURITY AND THE VACCINE DISTRIBUTION CHAIN

Facilities, especially vaccine mobile units, can take several simple, cost-effective steps to limit the exposure of their workers and the public to issues of loss, data, theft, or physical harm—including that from sUAS activity. **CISA recommends the following measures:**

- Back up critical data, ensuring copies of critical data are stored in the cloud or on an external storage device.
- Use multi-factor authentication and virtual private networks (VPNs). Implement automated border and host-level protections such as spam-filtering capabilities.
- Train workers through awareness training and simulations on preventing and reducing social engineering susceptibility, reporting incidents, and initiating incident response procedures.
- Only use secure networks, and avoid using public Wi-Fi networks.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Upgrade aging systems and replace end-of-support components—including software, firmware, operating systems, and hardware—when possible with supported and secure versions. When replacement is not possible, use network segmentation for vulnerable systems.

ℹ **For More Information:** Visit cisa.gov/cyber-essentials; Tip: Understanding Patches and Software Updates; Alert: Ransomware Activity Targeting the Healthcare and Public Health Sector; and CISA MS-ISAC Joint Ransomware Guide.

DEVELOPING AN EMERGENCY RESPONSE PLAN

Facility owners and managers can develop an Emergency Response Plan (ERP) with the help of CISA's Protective Security Advisors (PSAs). PSAs are critical infrastructure protection and vulnerability mitigation subject matter experts who can help state, local, and private sector officials conduct facility risk assessments.

- Explore CISA's emergency response training topics, including active shooter preparedness and insider threat awareness.
- Ensure local law enforcement and emergency responders are engaged in planning and exercise of ERPs.
- Take advantage of CISA's scalable templates, planning workshops, and functional exercises.
- Visit the Federal Emergency Management Agency (FEMA)'s Ready.gov site for guidance on creating and ERP, conducting a risk assessment, creating an evacuation plan, and including individuals with access and functional needs.

ℹ **For More Information:** Visit ready.gov/business/implementation/emergency, cisa.gov/protective-security-advisors, and cisa.gov/cybersecurity-training-exercises.

ADDITIONAL RESOURCES

COVID-19 Vaccine Physical Security Resources
cisa.gov/publication/covid-19-vaccine-physical-security

COVID-19 Vaccine Distribution Security Concerns in the Last Mile Infographic
cisa.gov/publication/covid-19-vaccine-distribution-security-concerns-last-mile

CISA Support to the COVID-19 Vaccine Rollout
cisa.gov/covid-19-vaccine-rollout

Physical Security Considerations for the Healthcare Industry During COVID-19 Response
cisa.gov/publication/physical-security-considerations-healthcare-industry-during-covid-19-response

COVID-19 Checklist: Securing Your Business and Clinical IT
cisa.gov/publication/covid-19-checklist-securing-your-business-and-clinical-it

Cybersecurity Resources for COVID-19
cisa.gov/cybersecurity-resources-covid-19

CISA Critical Infrastructure Exercises
cisa.gov/critical-infrastructure-exercises

FEMA's Emergency Management Institute
training.fema.gov/emi.aspx

Hometown Security
cisa.gov/hometown-security