Critical Questions and Considerations for Cold Chain, Storage, and Dry Ice Operations

December 2020

FINISHING STRONG

As we enter this "last mile" for COVID-19 vaccine distribution, numerous state and local planners have done diligent work to prepare for their custodial responsibilities. In support of these plans, and to ensure maximum realization of the COVID-19 efforts to date, CISA has developed critical questions and considerations that may inform and assist in further reducing risk to these life-saving efforts. These risks elevate the importance for the security and integrity of myriad of entities receiving, transporting, housing, and distributing COVID-19 vaccines. Any disruption to their delivery may impact public health, economic, and national security interests.

The following questions do not seek to be all encompassing nor replace your prior planning. Rather, a thorough reading aims to stimulate fresh ideas, new lines of critical thinking, and further self-assessment of your defensive posture. What follows is a list of recommended questions for state/local government officials, private sector entities, and cold storage facility owners/operators who will participate in the handling and distribution of COVID-19 vaccine related materials.

Cold Chain Availability and Logistics for Vaccines and Dry Ice

For State Vaccine Coordination:

1) What cold storage has been identified across the state to support rural distribution for locations that are multiple hours from major metropolitan areas, both for cold and ultra-cold (-80C)? Note: Different vaccines carry different cold requirements; please consult specific manufacturer handling requirements.
2) What process exists to verify total required capacity versus available capacity of cold storage units (to accommodate existing materials, vaccine contents, and/or transient dry ice)?
3) In case of refrigeration failure, who have you identified as alternative, contingent custodians of your supply of vaccines? And specifically, can they match your vaccine temperature requirements?
4) If you are dependent on dry ice, do you have contingency plans in case your primary is unavailable?

For Individual Cold Storage Facilities Preparedness:

1) What process exists to validate the accuracy and completeness of the asset inventory used in managing vaccines? What is the most recent date of the asset verification?
2) What capability exists to track and verify cold chain of custody?
3) Who are your facility's contacts with cold storage suppliers of assets necessary for cold operations?
4) What response plans have been developed if temperature does not hold or connectivity is lost?
5) If you are dependent on dry ice, do you have contingency plans in case your primary is unavailable?
6) Who are the relevant enterprise and computer/IT staff responsible for assisting with this effort?
7) What process exists to engage vaccine manufacturer(s) on the means to validate the integrity of vaccines?
8) Are there elements of the CISA Cold Storage Cyber Custodial Care information product that apply to your operations? If so, how have you addressed?
9) Do you have a notification process to ensure any questions or unplanned events are communicated to the appropriate stakeholders?
10) Do you have a physical security process for ultra-cold storage locations and refrigerated locations? (See additional physical and personnel security section below.)

Physical Security:

1) What is the physical security plan to protect the primary transport vehicles/drivers/delivery personnel in between the various state, county, jurisdictional locations? Includes prior to pick up (securing of trucks to prevent tampering of refrigeration units, injury to transport personnel, etc.), during transport, and at delivery.
2) Which types of security escorts will be utilized when transporting the vaccines from one place to another?
3) Do physical security plans include temporary storage locations, locking mechanisms, and storage devices?
4) What is the physical security plan for the final vaccine distribution locations, vaccination personnel, vaccines, kits, and persons being vaccinated?
5) What is the last date all stakeholders reviewed the facility and/or company's Physical Security Plan?
6) What is the last date all stakeholders reviewed the facility's and/or company's Emergency Action Plan?
7) Who are your federal, state, and local emergency and law enforcement contacts?
8) Are you aware, in addition to your state resources, CISA can assist with physical and cybersecurity assessments through their Protective Security Advisor (PSA) and Cybersecurity Advisor (CSA) programs?

Cyber/Infrastructure Resiliency:

1) What cold storage, HVAC, or physical security controls (like door locks) are integrated with OT, ICS, or SCADA systems? Have sufficient mitigations and/or defense in depth been employed?
2) What is the last date the facility tested its resilience to cyber threats, such as the one referenced in CISA's recent alert on cyber adversaries targeting cold chain facilities?
3) How long can the facility continue to operate normally (within range for temperature and time) if an adversary compromises and restricts access to the systems related to their cold storage equipment?
4) What capabilities exist for 24/7 monitoring capability, in-house or through a partner, to enable prompt detection and response to cyber threats?
5) What existing cyber threat intelligence sources are sufficient for maintaining vigilance? For example, is the facility receiving threat intelligence reports from CISA or a private sector source that can alert them on developments in threat landscape?

Personnel Security:

1) What is your process to verify proper authorization/authentication of personnel and third parties?
2) What is your process for employees to report unusual items/persons, or suspicious activity?
3) When was your most recent employee training on reporting insider threats?
4) When was the last time you reviewed basic security procedures (properly wearing badge, no follow through to locked/restricted units, emergency notification procedures)?

Incident Response Capabilities:

1) What were the results of the most recent incident response plan rehearsal? How recent was it? Note: If this process policy was written prior to COVID-19 telework and altered operations, has it been updated?
2) What capabilities exist to detect, respond, and recover to cyber incidents impacting vaccine integrity?
3) What were the results of the last recovery testing exercise? What was the date?
4) Who are the relevant IT staff responsible for assisting and/or executing response & recovery tasks?
5) What cybersecurity considerations are included in your business continuity/disaster recovery program? Is your BC/DR plan still sufficient?

CISA'S ROLE AS THE NATION'S RISK ADVISOR

As the Nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) leads the Nation's efforts to ensure the cybersecurity, physical security, and resilience of our critical infrastructure. CISA works with partners across government and industry to defend against today's threats and collaborates to build more secure and resilient infrastructure for the nation's Critical Functions.

Please visit the CISA COVID-19 Resource Page for more information. Victims of cold storage cyberattacks should report it immediately to CISA at Central@CISA.DHS.GOV, your local FBI Field Office or Secret Service Field Office. Federal and state assistance is also available through State Homeland Security Advisors and Emergency Management agencies.