Washington COVID-19: Supply Chain and Infrastructure Security Resources

December 2020

Overview:

The first shipment of COVID-19 vaccines arrived in Washington the week of Dec. 14, 2020. The following preparedness recommendations support the integrity and security of distributor facilities by addressing steps to mitigate cascading effects. Security threats include disruption to vaccine delivery, physical tampering to storage sites, and attacks against IT assets. The following preparedness measures are recommendations, and each provider must assess individual risk.

State and Local Guidance

- Update and confirm contact list for local, state and federal emergency and law enforcement.
- Sign-up for local Emergency Management Alerts –Contact Information here or here.
- Report anything suspicious (see something, say something) to your local law enforcement agency and the Washington State Fusion Center (WSFC) at: intake@wsfc.wa.gov
- Maintain situational awareness
    - Road conditions of delivery routes on Washington State Travel Alerts
    - Real-time major service outages that may disrupt communication Downdetector
- Contact cold storage power supplier and request to be added to priority power restoration list.
- Conduct health check of back-up generator.
- Host meeting with IT team to discuss potential attacks against IT assets – *refer to CISA Cold Storage Cyber Custodial Care*.
- Review Continuity of Operation (COOP) and Incident Response Plans (IRP) / Emergency Response Plan (ERP)

Federal Guidance

Department of Homeland Security – Cyber Security and Infrastructure Security Agency

- Cold Storage Cyber Custodial Care
- Critical Questions and Considerations for Cold Chain Storage, and Dry Ice Operations
- Physical Security for Cold Storage Locations
- Primer on Safe & Efficient Handling of Dry Ice

Additional Considerations

- Dry Ice and Liquid Nitrogen Can Cause Injuries or Death (PDF)