Ohio Homeland Security

1 June 2020

(U) Strategic Analysis & Information Center

(U) Physical Security Best Practices

(U//FOUO) Scope. Businesses should evaluate physical security measures to mitigate vulnerabilities and threats during teleworking and times when the area or building is not populated by employees or a security force.

(U//FOUO) Executive Summary

- The majority of the workforce in Ohio, and even throughout the United States, has shifted from in-office to telework virtually overnight. However, as economies begin to reopen and many stay at home orders have been lifted, the workforce will adjust again. It is critical to remind employees of physical security best practices when coming back to the office. Additionally, if your workforce continues to telework, it is important to maintain security procedures even when the majority of the staff are not coming into the office. Consider the physical security procedures below to mitigate vulnerabilities and reduce risk during this uncertain time.

    - *(U//FOUO) Daily Operations*
        - (U//FOUO) Ensure the facility locks away all documents containing personal identifying information and cash at the close of the business day.
        - Designate staff to check all doors and windows to ensure they are secured at the end of the business day.

    - *(U//FOUO) Hiring Practices*
        - (U//FOUO) Millions of individuals will be job searching and securing employment due to setbacks caused by recent events. Consider auditing hiring practices and establish policies and procedures to ensure criminal background checks are made on all employees, volunteers, interns, seasonal employees prior to hiring.

    - *(U//FOUO) Employee Training*
        - (U//FOUO) Since employees have been working from home the past few months, consider implementing a refresher training schedule to ensure the facility holds necessary training, such as shelter-in-place, active aggressor, and/or evacuation.

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) and contains sensitive information that may only be disclosed to individuals with a "right-to-know" & "need-to-know." Do not share this via unsecure internet servers or unencrypted email, and do not post within public view. This document must not be reclassified in any way and shall not be released to the public. Violation of these restrictions will be cause for removal from STACC/SAIC distribution lists.

- *(U//FOUO) Intrusion Detection Systems*
  - (U//FOUO) The premises should be protected by an intrusion detection system (i.e. interior motion detection, window and door contacts) to mitigate vulnerabilities in the evening hours.
  - (U//FOUO) If an intrusion detection system is present at the facility, the alarm arming and de-arming codes should be changed frequently. Consider changing these codes if employees have left the agency and are not expected to return to work due to the pandemic.

- *(U//FOUO) Key Control*
  - (U//FOUO) Establish policies and procedures to ensure key audits are conducted regularly, especially with employees returning to the office from teleworking.
  - (U//FOUO) Consider changing keys and locks if employees have left the agency and are not expected to return to work.

- *(U//FOUO) Building Envelope- Doors and Windows*
  - (U//FOUO) With limited staff in the building in the transition from teleworking, ensure all exterior doors outside of the main entrance are locked during business hours.
  - (U//FOUO) Ensure doors and windows are fitted with quality locks to restrict tampering and access.
  - (U//FOUO) Landscaping may have been unavailable due to current events. Shrubs and landscaping should be cut to the base of the windows or low enough to negate concealment.

- *(U//FOUO) Perimeter Security*
  - (U//FOUO) If the agency is partially or fully enclosed in fencing, evaluate the fence structure for damage, such as holes in a chain-link fence, and repair any damage found.
  - (U//FOUO) Consider exploring the feasibility of installing passive motion sensors around critical equipment to monitor activities as an additional security measure.

- *(U//FOUO) Video Security*
  - (U//FOUO) If the agency uses a closed circuit television (CCTV) system, consider evaluating the equipment to ensure camera images are recorded for at least 30 days, can identify individuals on the property, and ensure there is emergency backup power for cameras. Additionally, criminals may exploit a facility known to not have many employees in the building due to recent events. Ensuring the camera equipment is up-to-date will strengthen security practices and mitigate this risk.

(U) Questions on this Product

(U) If you have any questions regarding this product, please contact the Critical Infrastructure Unit at (844-647-2467) or email at SAICIP@dps.ohio.gov.

(U) Report Suspicious Activity

(U) Please report any suspicious activity to (877) OHS-INTEL (647-4683) or to STACC@dps.ohio.gov.