Work from Home Guidelines for Secure Enclaves (COVID-19)

Background

The purpose of this document is to outline guidelines for a work from home situation that is encouraged or required in the event of the current pandemic (COVID-19). This document applies to all campuses, colleges, units, and departments which work with level 3 or 4 data inside a secure enclave with an approved Authority to Operate.

Up to date information on the University’s overall response to COVID-19 can be found at https://sites.psu.edu/virusinfo/

Restrictions

Certain data sets may have obligations through contract, system security plan, or other mandate that places restrictions on where the data can be physically viewed at. For these data sets, a work from home situation cannot be accommodated. Also, some level 3 and 4 data elements have high risk implications with them that do not allow the data to be accessed in a work on from home situation. These decisions are all handled by the Privacy, Risk, and Compliance team within OIS. Finally, data sets that have true NIST 800-171 compliance requirements tied to them will need an alternative VPN provided which supports full-tunnel VPN. The current Penn State VPN is only capable of split-tunnel connections and therefore does not meet NIST 800-171 compliance.

Before allowing any level 3 or 4 data to be worked on from home, you must consult with OIS.

General Requirements

If level 3 or level 4 data is deemed to be allowed to be worked on from home by OIS, the following requirements must be met:

- The ATO must have full approval or be in a provisional state.
- All data within the enclave is accessed via Penn State VPN.
- Penn State provided computers must be used to access the data from home.
  - Personal devices are not allowed at this time.
- Splunk, Cylance, and Nessus (all RHS) must be installed on the devices connecting from home.
- The systems must be part of Enterprise Active Directory (EAD)
Personally Owned Device Concerns

At this time, no personally owned devices should be used to access level 3 or 4 data. This applies to all situations and ATO types regardless of ATO configurations in place including jump servers, bastion hosts, CyberArk, restricted data transfer functions, etc. Personally owned computer cannot be guaranteed as secure and still leave enclave access susceptible to:

- Common exploits including RDP exploits from not being regularly patched.
- Unknown malicious applications that the user has installed.
- Operating systems that no longer have security updates provided by the vendor.
- Remote Access Trojans (RAT) which allow attackers to have complete control of the system unknown to the user.
  - This would include ability to view screens and, in some cases, control them over RDP sessions.
  - These allow complete file transfer capabilities.
- Keylogger applications which capture user keystrokes.
  - User keystrokes would include usernames, passwords, and potential level 3 / 4 data elements.

Remote Enclave Access Process

If you have a legitimate business need to access an enclave from home, please use the following steps:

1. Email security@psu.edu with the LR number of the enclave that needs to be accessed from home. Please give detailed information and business justifications so that we can understand the full context of the request and consider all the impacts.
   a. Ensure that devices being taken home for enclave access can meet the information in the “General Requirements” section of this document.
2. A member of the OIS Consulting & Architecture team will coordinate with OIS Privacy, Risk, and Compliance to determine if it is acceptable for the data to be accessed out of its normal work environment.
3. If allowed, you will be notified. We will track that the enclave is being accessed from home and note the LR.
4. You will work normal enclave and firewall channels to get the data accessible over the VPN.
   a. You are required to inform us immediately if the situation changes and the data no longer needs accessed from home.
   b. As soon as the work from home need ends you will immediately need to cut off the external VPN access through normal enclave and firewall channels.