COVID 19 and the support of Remote Work Environments for Law Enforcement in Texas

CJIS Guidance for Texas Law Enforcement Agencies and Personnel

Our law enforcement personnel and services are critical to everything we do in providing responses to emergencies and our local communities, friends and family. In our efforts to lessen the impact in as much as we can and continue to provide the level of service and support necessary, we often rely on technology. Web-based applications, portals and conferences allow us to provide easy and readily available resources for our communities. However, in light of supporting POTUS and Governor Abbott's guidance in addressing the limitation of travel and social space to limit any spread or worsening of this pandemic, we must implement remote work capabilities where possible. As law enforcement, charged with protecting and processing highly sensitive information we want to remind all law enforcement of the requirements and responsibilities unique to our data and systems.

Requirements include the FBI CJIS Policy, the CFR Title 28, Part 20 and the Texas Government Code Chapter 411 among other legislative and local policies.

Below are a few tips and helpful resources specific to law enforcement within our state. This is being provided as guidance only. It is a high-level overview of key areas that should be considered but nothing should be used to subvert or supersede any local agency policy or process that may be available. We encourage all users to ensure they have discussed remote access and use with your local agency executive staff prior to attempting to work on sensitive data or systems remotely.

TELECOMMUTING TIPS FOR LAW ENFORCEMENT WITHIN TEXAS

1. **Identify equipment needs and resources.**
   Ensure the agency has available resources, equipment and capability to support remote work.
   a. Identify the personnel, which may be considered for Work From Home (WFH).
   b. Identify the equipment needs; laptop, handheld devices, etc.
      Note: For Criminal Justice, all devices connecting to the agency's network should be agency issued. It is never recommended to allow personal devices to access a secure criminal justice environment.
   c. Ensure the personnel have access to a private network (Home network, WiFi that supports a minimum of WPA2 standards or a wireless hotspot is being used which is assigned to the individual and requires a passcode to join). (CSP 5.13.1.1)
      Note: Free WiFi hotspots such as those found in public spaces, coffee shops, etc. should never be used to establish connections into criminal justice agency networks.
   d. Ensure the connection is being established through an approved and secure encrypted tunnel (VPN). The encrypted tunnel shall meet the in-transit encryption requirement of FIPS 140-2.
   e. For remote work involving a connection outside of the secure location, consider whether there is an approved Advanced Authentication (AA) or 2 Factor / Multifactor authentication being used.

f. For mobile solutions, agencies must include a Mobile Device Management (MDM) solution for tablets and smartphones. (CSP 5.13.2)

2. Protect and secure equipment and data

Where will the remote work be conducted? Is the remote space in an area that can be controlled in a manner to prevent unauthorized viewing of sensitive or CJI data? Can the area be secured when you are unavailable?

a. Ensure you treat all information at appropriate levels, regardless of location we are ultimately responsible for the protection of sensitive data. Be wary of your surroundings, who may be in the area and who may be looking over your shoulder. This includes family members in at home environments. You want to ensure your workspace is secure in the same manner you would consider your office space at work.

3. Protect the Information

Using remote devices always involve resident data.

a. Protect the equipment and tools; secure them in a locked cabinet, etc. when you are not in the area. This includes printed material or hard copy documents, if you are using remote equipment you should be mindful of who may come into contact or exposed to the material.
b. For digital material, this should be encrypted at appropriate levels. For data at rest, this would require a minimum of AES 256 or FIPS Level 197. This requirement would apply to hard drives, removable USB drives and discs. (CSP 5.10.1.2.2)
c. Data in transit is required to be encrypted at a minimum of FIPS level 140-2 encryption.

4. Bring your own device (BYOD) and Publicly Accessible Devices

The FBI CJIS Security Policy requires any agency involved in accessing or processing CJI should have established local policies which address appropriate usage of equipment. (CSP 5.5.6.1)

a. Consideration involving any allowed use of personal devices should be documented in advance and expressly address how any equipment involved with CJI is to be managed, protected, including patching and updates, antivirus and malware protection, etc.
   NOTE: As stated above it is never a recommended practice to allow use of personal devices due to the potential loss of personal information, litigation issues involving personal property and the lack of agency controls to administer and manage such devices. At any time, BYOD is being considered we encourage the agency to reach out in advance for assistance in establishing appropriate controls and documented policies in meeting the requirements of the CSP.
b. Publicly accessible computers shall not be used to process, store or transmit CJI. (CSP 5.5.6.2)

5. Training and Good Security Practices

Ensure all staff who may be considered for remote work are up to date on effective security awareness training. (CSP 5.2)

a. There are varying levels of Security Awareness which are identified within the CSP. These are specific to the level of access and job function.
b. Additionally, knowledge and reminders of common cyber-attacks and best practices related to effective online security is vital.
c. If nearing password expiration, consider changing and testing passwords before working remotely as it may be difficult to change later at a remote location.

d. Ensure users are familiar with reporting requirements and know who to contact for security incidents and what is expected regarding agency devices and usage. The CSP requires Incident Reporting for any loss or compromise of criminal justice information including any device, which stores, processes or accesses CJI.

This is presented as a high-level overview of the areas of concern involving work from home. We encourage agencies to reach out to us in advance to assist in the development of appropriate policies and controls involving remote use as it relates to criminal justice information and systems. The CJIS Technical Auditor Team is available to assist the agency in the development of policies, provide samples of the required documentation, as well as support and provide guidance for any network or technical issues relating to CJIS.

"Other" Communication methods

Law enforcement must remain cautious when considering third party solutions related to information sharing and communications. Additional resources and methods in regards to maintaining communications is the FBI's Law Enforcement Enterprise Portal (LEEP) at https://www.cjis.gov for secure communication services. This is a valuable resource and includes the Virtual Command Centers (VCC) and Justice Connect. The solution allows secure Communities of Interest (COI) to be created for the agency, section, or unit to allow exchange of files, discussion boards, and real time chat interfaces for law enforcement.

During these stressful events and times such as the COVID-19 Pandemic it is important for law enforcement to remember bad actors seek out and leverage reduced or stressed resources as prime times to launch and attempt cyber-attacks. Within Texas, we have experienced first-hand the havoc and damage that can result from a single source attack targeted against our communities. We need to remain alert and knowledgeable in common tactics using links and attachments in emails, messages, and online – this is especially true as it relates to devices and equipment being utilized in a remote environment. The key to any deployment of a remote work strategy involves ensuring timely patches and updates and the ability to manage or control the device(s). The most common incident involving remote use involves the loss or compromise of the device; lost, stolen, etc.

Ultimately, remote work can be an effective use of resources, both from an agency perspective as well as for each of us individually. It can be leveraged in times of need to continue services in an uninterrupted state for many of the tasks and responsibilities agencies perform on a daily basis. Ensuring all remote personnel are effectively prepared and equipped should also include consideration for messaging and collaboration for continuity and effective communication with peers, supervisors and daily interactions. A reminder that any remote connection broadens our borders of the secure network and relevant knowledge of good online security practices is critical.

Be healthy and safe, the people in Texas depend on you.

Other helpful links:

The FBI Criminal Justice Information Services (CJIS) Policy Resource:

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/fbi-cjis-security-policy-resource-center-links-of-importance

For Texas CJIS Security Awareness Training Online

https://www.cjisonline.com

NIST Guide to Remote Working

https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

The Office of Personnel Management (OPM) has helpful ideas and tips for manager and agency responsibilities:

https://www.telework.gov/guidance-legislation/telework-guidance/emergency-telework/

Microsoft offers some tips to CISOs on implementation of remote work:

https://www.microsoft.com/security/blog/2020/03/12/support-working-from-home-securely/