Maintaining CJIS Compliance While Working Remote

POC: John C. "Chris" Weatherly, FBI CJIS ISO iso@fbi.gov

Executive Summary: When developing plans for continuity of operations during situations that may necessitate remote work arrangements, agencies may consider having some employees work from locations outside of the agency's physically secure location. When considering alternative work options requiring physical or logical access to unencrypted criminal justice information *(CJI)*, agencies should be mindful of CJIS Security Policy requirements and the need to protect CJI at all times.

Introduction: With the latest news and advice from the Centers for Disease Control *(CDC)* and government authorities on the COVID-19 pandemic, agencies may consider having some employees work from home. Per the Federal Bureau of Investigation's Criminal Justice Information Services *(CJIS)* Security Policy, *(CJI)* must be protected at all times. Agencies should decide if having individuals working from home with physical or logical access to unencrypted CJI is appropriate. Agencies can employ stricter policies than are listed below. Agencies should review their policies to see under which scenarios working from home is appropriate and which positions are authorized. Reporting security incidents for unauthorized access to CJI including unauthorized transfer of CJI to a non-agency device *(data spills)* should also be included.

Personnel Security: Per CJIS Security Policy Section 5.12, individuals having physical or logical access to unencrypted CJI must successfully complete a fingerprint-based record check by the criminal justice agency. This also applies to non-criminal justice agencies having the authority to screen individuals. For those without the necessary authority, access should be limited to those with an operational need to access CJI. Unauthorized individuals *(family members, roommates, etc.)* are not permitted to view CJI or operate devices that contain or can access CJIS.

Security Awareness Training: Individuals accessing CJI must have the proper level of security awareness training depending on their job function and level of access. CJIS Security Policy Area 5.2 has the different levels of training.

Publicly Accessible Devices: Per CJIS Security Policy 5.5.6.2, publicly accessible computers shall not be used to access, process, store, or transmit CJI. Make sure your employees know that they cannot use computers in libraries, hotel lobbies, schools, etc., for working with CJI.

Personal Equipment: A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices *(i.e. bring your own device [BYOD])* are authorized, the device shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

Limited and Full-Featured Operating Systems: Devices with a limited feature operating system must include a Mobile Device Management *(MDM)* solution. See policy area 5.13.2 for MDM requirements. Full-featured operating systems must have anti-virus software and a personal firewall enabled.

Home Networks: An employee may connect to his/her home Wi-Fi or 'hotspot' on a personal phone if it requires a passcode to join. Wi-Fi networks without passcodes are not secure and should not be used. Similarly, wireless printing is not secure and so should not be used. Connections to a home printer should be with an applicable cable. Printing to a public printer is not allowed. If possible, CJI or sensitive materials should not be printed while outside of the agency's physically secure location.

Creating a Controlled Area: Remote employees must designate areas where CJI is stored or processed as a controlled area to properly protect CJI. In a home environment, individuals must take necessary precautions to protect CJI. At a minimum, remote employees must:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

Identification and Authentication *(Advanced Authentication)*: Individuals that have physical or logical access to unencrypted CJI must be uniquely identified with a username and a password that meets policy. Advanced Authentication *(AA)* is required for direct access to CJI from outside of the agency's physically secure location. Direct access is the ability to query or update state and national databases including those maintained by the State and the FBI. Accessing criminal history results previously received from the State for applicant purposes *(employment, licensing, etc.)* is considered indirect access and AA is not required.

Encryption in Transit AND at Rest: If a device contains unencrypted CJI, the data must be encrypted if the device can operate outside of the agency's physically secure location. When encryption is employed, agencies shall use a symmetric cipher that is FIPS-197 certified Advanced Encryption Standard *(AES)* and at least 256 bit strength. When CJI is transmitted outside the boundary of the physically secure location, the data must be encrypted using a cryptographic module that is FIPS 140-2 certified and uses a symmetric cipher key strength of at least 128 bit strength. Virtual Private Network *(VPN)* users shall only use a CJIS Systems Agency *(CSA)* approved VPN solution.

Increased Vigilance: The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user *(or an information system)* communicating temporarily through an external, non-agency-controlled network *(e.g., the Internet)*. The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Incident Reporting: The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

Criminal Justice Information Spills: The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed *(cut up, shredded, etc.)*. The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.