California Department of Justice
CALIFORNIA JUSTICE
INFORMATION SERVICES DIVISION
Joe Dominic, Chief/CJIS ISO

INFORMATION BULLETIN

Subject:	*No.*	*Contact for information:*
Maintaining CJIS Compliance While Working Remotely	20-06-CJIS	CLETS Administration Section (916) 210-4240 cas@doj.ca.gov
	Date: 04-08-20	

TO: ALL CRIMINAL JUSTICE AGENCY PERSONNEL, AGENCY HEADS, FCIC AGENCY COORDINATORS, LOCAL AGENCY SECURITY OFFICERS, CJIS AGENCY COORDINATORS

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 (e.g. data electronically presented on a computer or mobile device) to unencrypted criminal justice information (CJI), agencies should remain mindful of the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy (FBI CSP) requirements and the need to protect CJI at all times.

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. Agencies should decide if having individuals working from remote locations with physical or logical access to unencrypted CJI is appropriate. The following are the FBI CSP security controls that agencies should consider when allowing remote work arrangements that require access to CJI:

Creating a Controlled Area (FBI CSP 5.9.2)

Agencies must designate areas where CJI is stored or processed as physically secure locations or controlled areas to properly protect CJI. In a home environment, individuals must take necessary precautions to protect CJI. At a minimum, agencies should evaluate each situation to see if it meets the criteria for a controlled area, including locking any device used to store or view CJI when not in use and positioning devices containing CJI in a manner so as to prevent unauthorized access and view.

Printed documents containing CJI should not be removed from an agency's physically secure location if possible. If absolutely necessary, printed CJI should be stored in a locked storage container when left unattended and should not be viewed or accessed by unauthorized individuals (FBI CSP 5.8.2.2).

Personal Equipment (FBI CSP 5.5.6.1)

A personally-owned information system (e.g. personal computer, personal smart phone, etc.) 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 FBI CSP Policy Area 13: Mobile Devices.

When facing an employee's extended leave, quarantine, or other work-from-home necessity, the easy answer may be to allow the employee to access agency resources from his/her own computer. This is not forbidden by CJIS policy, but the agency must be able to enforce terms and controls for the device (FBI CSP 5.13, and Appendix G.4). FBI CSP recommends that the agency have the employee sign a waiver or declaration of understanding prior to allowing the employee to access agency resources from his/her personally-owned devices. FBI CSP also recommends that the agency prohibit employees from saving any CJI to their personal devices to avoid associated CJIS obligations (encryption at rest, hard drive sanitization, etc.). For mobile devices that access CJI directly and have limited operating systems (e.g., phones and tablets), Mobile Device Management is required (FBI CSP 5.13.2). The same is true for personally-owned devices. It may be difficult to implement these controls on short notice, and employees may object to these controls on their personal devices (for example, their agency would need to be able to track the location of the device, or the employee would have to surrender the device to the agency when employment ceases so the agency can properly destroy or sanitize the device).

In short, while there are ways for employees to access CJI on personal phones or mobile devices while staying in compliance with FBI CSP, however, it is critical that the FBI CSP controls and limitations are understood and implemented

Home Networks (FBI CSP 5.13.1.4)

An employee may utilize his/her home Wi-Fi or 'hotspot' to connect remotely to the agency network as long as it is password-protected with a secure, complex password (e.g. password includes upper and lower case letters, numbers, and symbols). Wi-Fi networks without passcodes are not secure and should not be used.

If possible, CJI or sensitive materials should not be printed when outside of the agency's physically secure location. If printing is necessary, a public printer should not be used. Only home printers with applicable cables should be used, as wireless printing is not secure and should not be used. If CJI is printed, it should be stored in a locked container when left unattended to avoid unauthorized access, view, and use.

Identification & Authentication (Advanced Authentication)

Individuals with physical or logical access to unencrypted CJI must be uniquely identified with a username and a password that meets FBI CSP policy. Advanced Authentication (AA) is required for direct access to CJI from outside of the agency's physically secure location (FBI CSP 5.6.2.2). Direct access is the ability to query and update state and federal databases, including those maintained by the CA DOJ and the FBI. Accessing criminal history results previously received from the CA DOJ for applicant purposes (employment, licensing, etc.) is considered indirect access and AA is not required.

Encryption in Transit and at Rest (FBI CSP 5.10.1.2)

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 (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.

Personnel Security (FBI CSP 5.12)

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

Security Awareness Training (FBI CSP 5.2)

Individuals with access to 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 sets forth the different levels of training.

Agency Policies

Agency management should review their agency policies to familiarize themselves with the situations that require and the positions that are authorized for alternative work arrangements. Procedures for reporting security incidents related to unauthorized access to CJI and unauthorized transfer of CJI to a non-agency device (data spills) should also be included.

Publicly Accessible Devices (FBI CSP 5.5.6.2)

Publicly accessible computers shall not be used to view, access, process, store, or transmit CJI. Ensure agency employees know that they may not use computers in libraries, hotel lobbies, schools, etc., when working with CJI.

Increased Vigilance

Agencies 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). Agencies shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. Agencies shall control all remote accesses through managed access control points. Agencies may permit remote access for privileged functions only for compelling operational needs, but shall document the technical and administrative process to enable remote access for privileged functions in the security plan for the information system.

Incident Reporting (FBI CSP 5.3.1)

Agencies shall promptly report incident information to the CLETS Administration Section (CAS) at

(916) 210-4240 or via email to cas@doj.ca.gov. Security events, including identified weaknesses associated with the event, shall be communicated in a manner to allow for timely enforcement of corrective action. Formal event reporting and escalation procedures shall be established and maintained. Wherever feasible, agencies 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.

If you have questions, please contact the CLETS Administration Section at (916) 210-4240 or cas@doj.ca.gov.

Sincerely,

Joe Dominic

JOE DOMINIC, Chief/CJIS ISO
California Justice Information Services Division

For XAVIER BECERRA
Attorney General