



## Police Department

---

Date: November 30, 2018

To: Richard Mason  
Department of Justice, CLETS Administration Section

*Via email to [Richard.Mason@doj.ca.gov](mailto:Richard.Mason@doj.ca.gov)*

Re: **FBI ITS Quarterly Audit CLETS Compliance Technical Report**

Dear Mr. Mason:

The Chula Vista Police Department is actively working to resolve all issues indicated in our previous implementation plan to become compliant with the FBI CJIS Policy in its entirety.

The following are technical items that have been resolved with completion dates and steps taken along with items that are still in progress with their targeted completion dates and steps being taken:

1. **System Use Notification:** *Chula Vista Police Department has not ensured that local agencies display an approved system use notification message on all information systems accessing Criminal Justice Information (CJI).*

**Status: RESOLVED, approximately February 1, 2018**

**Steps taken:** Shortly after completion of the audit, new information technology protocols were implemented to resolve this issue. All information systems that access CJI now display a system use notification message as required, along with requiring the user to acknowledge the message before accessing the system.

2. **Encryption:** *The Chula Vista Police Department was unable to provide verification that CJI accessed at their data center, which was not a physically secure location, was encrypted at rest with at least 128-bit NIST certified encryption.*

**Status: RESOLVED on October 29, 2018**

**Steps taken:** We have decommissioned and removed the servers and storage from the non-secure data center at the city IT facilities. We have replaced those with new servers and storage within the secure police department headquarters facility including CJIS compliant 128-bit encryption.

3. **Supplemental:**

- a. *The Chula Vista Police Department allowed the use of publicly accessible computers to access, process, store, or transmit CJI.*

**Status: RESOLVED, approximately July 1, 2018**



## Police Department

---

**Steps currently being implemented:** Our Information Technology unit implemented new security measures to assure that any publicly accessible computers do not have access to our department network, and cannot process, store, or transmit CJI. A new computer was installed on a guest Internet connection for the public to use. The previous computer is secured to only allow authorized agency personnel to login.

- b. The Chula Vista Police Department does not authorize, monitor, and control wireless access to information systems containing CJI.*

**Status: RESOLVED, approximately October 1, 2017**

**Steps taken:** At the time the audit was conducted, our agency had begun issuing new wireless devices to agency personnel. But we had yet to allow those wireless devices to access information systems containing CJI, and therefore had yet to implement tools and controls to authorize, monitor, and control access to said systems. Since that time, however, our agency has further implemented wireless devices practices and now maintain multiple management systems to authorize, monitor, and control wireless access to information systems containing CJI. These management systems include, for example, NetMotion for authentication and monitoring of Virtual Private Networking (VPN), Microsoft InTune's Mobile Device Management (MDM) for mobile device control, and a variety of other monitoring tools and controls for specific systems such as the agency's Computer Aided Dispatch (CAD) system.

- c. The Chula Vista Police Department does not implement procedures to disable wireless devices if lost or stolen.*

**Status: RESOLVED, approximately October 1, 2017**

**Steps taken:** At the time the audit was conducted, our agency had begun issuing new wireless devices to agency personnel. But we had yet to allow those wireless devices to access information systems containing CJI, and therefore had yet to implement procedures to disable the devices if lost or stolen. Since that time, however, our agency has fully implemented Mobile Device Management (MDM) and has since implemented procedures to disable wireless devices if lost or stolen.

We here at the Chula Vista Police Department worked diligently to resolve all issues listed in our 2017 audit and strive to be completely compliant with all FBI CJIS requirements.

We truly appreciate all your help and guidance to get our Department in compliance. If you have any questions, please feel free to contact our current Agency CLETS Coordinator, Shannel Honore at (619) 476-2310 or [shonore@chulavistapd.org](mailto:shonore@chulavistapd.org).

Respectfully,

Roxana Kennedy  
Chief of Police