



COUNTY OF SAN MATEO
OFFICE OF THE SHERIFF

CARLOS G. BOLANOS
SHERIFF

MARK C. ROBBINS
UNDERSHERIFF

400 COUNTY CENTER REDWOOD CITY CALIFORNIA 94063-1662 TELEPHONE (650) 599-1664 www.smcsheriff.com

ADDRESS ALL COMMUNICATIONS TO THE SHERIFF

December 4, 2019

Ms. Maria Cranston
CLETS Executive Secretary
California Department of Justice
P.O. Box 903387
Sacramento, CA 94203-3870

Re: Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division,
Information Technology Security Audit (ITSA) Report

Dear Ms. Cranston:

Please see our response in green below to The FBI's audit.

1. **Security Addendums:** The San Mateo County Sheriff's Office received IT services from Raging Wire. However, FBI CJIS Security Addendums were not signed and maintained for these personnel.

San Mateo County Sheriff's Office will be compliant by July 15, 2019. Fingerprints, security addendums, and private management control agreements will not be necessary for Raging Wire as they will have no physical access to BMI's cage under any circumstance, even in an emergency. BMI will install electronic badge controlled locks on all the equipment cabinets and only BMI staff will have access. This will be completed by July 15, 2019.

Controlled badge access was added 07/17/19 to BMI cabinets located at Raging Wire so that only BMI employees have access.

2. **Personnel Security:** The San Mateo County Sheriff's Office did not fingerprint all Raging Wire personnel with unescorted access to criminal justice information (CJI.)

San Mateo County Sheriff's Office will be compliant by July 15, 2019. Fingerprints, security addendums, and private management control agreements will not be necessary for Raging Wire as they will have no physical access to BMI's cage under any circumstance, even in an emergency. BMI will install electronic badge controlled locks on all the equipment cabinets and only BMI staff will have access. This will be completed by July 15, 2019.

Controlled badge access was added 07/17/19 to BMI cabinets located at Raging Wire so that only BMI employees have access.

3. **Security Awareness Training:** The San Mateo County Sheriff's Office did not Raging Wire private contractor personnel, who managed or had access to CJI, received security awareness training.

San Mateo County Sheriff's Office will be compliant by July 15, 2019. Fingerprints, security addendums, and private management control agreements will not be necessary for Raging Wire as they will have no physical access to BMI's cage under any circumstance, even in an emergency. BMI will install electronic badge controlled locks on all the equipment cabinets and only BMI staff will have access. This will be completed by July 15, 2019.

Controlled badge access was added 07/17/19 to BMI cabinets located at Raging Wire so that only BMI employees have access.

4. **Physical Security:** The San Mateo County Sheriff's Office is in the process of digitizing old case files, containing CJI, to an internet-based interface, called Digital ReelL, maintained by a third party vendor, called BMI Imaging Systems. CJI data is stored in two locations; the first, is maintained by the unauthorized contractor BMI Imaging Systems (located at 1115 East Arques Avenue, Sunnyvale, California). The second location is a sub-contracted facility, maintained by Raging Wire, an unauthorized third party (located at 1200 Striker Avenue, Sacramento, CA). Both contractors have unescorted access to unencrypted CJI without proper authorized of the criminal justice agency which includes a fingerprint-based record check, signed CJIS Security Addendum (for each individual contractor with access), and evidence of completed security awareness training (within 6 months of access and every 2 years).

San Mateo County Sheriff's Office will be compliant by July 15, 2019. Fingerprints, security addendums, and private management control agreements will not be necessary for Raging Wire as they will have no access to BMI's cage under any circumstance, even in an emergency. BMI will install electronic badge controlled locks on all the equipment cabinets and only BMI staff will have access. This will be completed by July 15, 2019.

BMI Sunnyvale location is compliant.

Controlled badge access was added 07/17/19 to BMI cabinets located at Raging Wire so that only BMI employees have access.

5. **Authentication:** The San Mateo County Sheriff's Office was unable to verify that passwords used to access Tiburon RMS and ATIMS application passwords did not comply with any secure password attributes.

ATIMS has been compliant since December 2018.

San Mateo County Sheriff's Office will be compliant by September 2019. BMI is currently converting our Tiburon database. This will be completed by September 2019. Once this is complete we will shut off our legacy system Tiburon..

We anticipate being able to decommission, Tiburon, our legacy system by December 2019.

Our legacy system Tiburon will be decommissioned on our target date of December 16, 2019.

6. **Event Logging:** BMI Imaging Systems – Digital ReelL: The San Mateo County Sheriff's Office utilized an information system, maintained by BMI Imaging Systems, which did not log successful and unsuccessful log-on attempts.

BMI has confirmed they review log-in attempts and log all unsuccessful attempts.

We anticipate being able to decommission, Tiburon, our legacy system by December 2019.

Tiburon RMS: In addition, the Tiburon RMS, a legacy RMS containing CJI, did not log successful and unsuccessful password changes, successful log-on attempts, or successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other system resource. The Tiburon RMS did not provide alerts to agency officials if/or when an audit processing failure occurs. Lastly, the agency did not review their system audit logs for the Tiburon RMS, at a minimum of once a week, for inappropriate, unusual, or suspicious activity.

San Mateo County Sheriff's Office will be compliant by September 2019. BMI is currently converting our Tiburon database. This will be completed by September 2019. Once this is complete we will shut off our legacy system Tiburon.

All of our data has been converted from our legacy system (Tiburon), into Digital Reel (BMI) and we are in the process of verifying the accuracy of the converted records. We anticipate being able to decommission our legacy system, Tiburon, by December 2019.

7. **Advanced Authentication:** The San Mateo County Sheriff's Office was unable to provide details or verify the use of advanced authentication for internet-based access to Coplink, a direct access information system, by users or by IT administrators performing maintenance on the system.

In order for a user to access Coplink all the following must be true:

- ☐ The computer being used must be on the Sheriff's Office secured network.
- ☐ The user must have a user account on the Sheriff's Office Windows Domain.
- ☐ The user must be able to successfully log onto a Sheriff's Office computer.
- ☐ The user must have credentials to log onto Coplink.

San Mateo County Sheriff's Office will be compliant by December 2019. This is a large roll out for all county agencies, The Sheriff's Office is on our own network causing additional work. We will use OKTA. You need a password and text or email pin that authenticates to our network to access our network.

We will not be compliant by our target date of December 2019. This project has been extended by six months. We believe we will be compliant by June 2020.

Coplink is only accessible from the Sheriff's Office Network.

The Sheriff's Office still anticipates completion by our original target date of December 2019.

Coplink issues were resolved in a closed door CAC session.

8. **Encryption:** The San Mateo County Sheriff's Office was unable to provide a FIPS

140-2 certificate associated with website delivery of CJI via Digital ReelL (maintained by BMI Imaging Systems). In addition, the contractor BMI Imaging Systems is using a dedicated fiber between datacenter locations (1115 East Arques Avenue, Sunnyvale, California and 200 Striker Avenue, Sacramento, CA). Neither the CJI nor the network segment are encrypted between datacenter locations. Furthermore, the contractor, BMI Imaging Systems, was unable to provide requested information in reference to remote capability of IT administrators from outside the datacenter (remote maintenance capability). Lastly, CJI was stored at rest outside of a physically secure location (both datacenters contained unauthorized personnel with access to the facility – Raging Wire and BMI Imaging Systems personnel are not authorized) without encryption. The San Mateo County Sheriff's Office was unable to provide the details of the method of encryption or provide a FIPS 140-2 certificate associated with website delivery of CJI via Coplink (maintained by IBM with direct access to N-DEx). In addition, the agency did not provide any requested information in reference to encryption methods for remote maintenance by IT administrators of IBM or back-ups of CJI maintained within Coplink.

Certificates have been provided to DOJ.

Resolved at closed door CAC Session

Sincerely,

Carlos G. Bolanos, Sheriff

A handwritten signature in blue ink, appearing to read 'Mark C. Robbins', with a stylized, flowing script.

By: Mark C. Robbins, Undersheriff