

**CRIMINAL AND JUVENILE JUSTICE INFORMATION SYSTEMS
(CJJIS) COUNCIL**

**MINUTES OF MEETING
Tuesday, March 28, 2023
Video Conference**

Members Present:

Mike Prendergast, Sheriff, Citrus County Sheriff's Office

Roosevelt Sawyer, Jr., Designee for Ali Sackett, Office of the State Courts Administrator (OSCA)

Carolyn Timmann, Martin County Clerk of Circuit Court and Comptroller

Chuck Murphy, Designee for Commissioner Mark Glass, Florida Department of Law Enforcement (FDLE)

Gina Giacomo, Designee for Melinda N. Coonrod, Chair, Florida Commission on Offender Review (COR)

Giri Vasudevan, Designee for Shevaun Harris, Florida Department of Children and Families (DCF)

Charles Broadway, Chief, Clermont Police Department

Doug Smith, Designee for Attorney General Ashley Moody

Members Absent:

R.J Larizza, State Attorney, 7th Judicial Circuit

Tim Roufa, Designee for Executive Director Dave Kerner, Department of Highway Safety and Motor Vehicles (DHSMV)

Stacy A. Scott, Public Defender, 8th Judicial Circuit

WELCOME MEMBERS and OPENING

Chair Prendergast called the meeting to order at 9:32 a.m. and introduced CJIS Director Lucy Saunders. Chair Prendergast requested a motion to approve the November 29, 2022 CJJIS Council Meeting minutes. Council Member Timmann moved and Council Member Sawyer seconded the motion to approve the November 29, 2022 minutes. The motion passed.

ITEM 1

Florida Sunshine Law

Assistant General Counsel Janine Robinson

Florida Department of Law Enforcement

Information and Discussion

Chair Prendergast recognized Assistant General Counsel Janine Robinson who briefed the Council on the Florida Sunshine Law requirements. Assistant General Counsel Robinson stated "The Sunshine Law," Florida Statutes Chapter 286 was enacted in 1967. Florida has one of the *most expansive* open government and public records laws in the Nation, and it stipulates no government decisions should be made behind closed doors.

There are three basic requirements:

- 1) Meetings of any board, commission, or council **must** be open to the public;
- 2) Reasonable notice of meetings **must** be given; and
- 3) Meeting minutes **must** be taken and available, by request, in a reasonable time.

If two or more members meet, telephone, exchange an email or text regarding a topic that may foreseeably come before the Council for action, then that exchange falls within the parameters of the Florida Sunshine Law. On the public records side, FDLE has noted an increased number of records requests for text messages. Assistant General Counsel Robinson recommended if you do not have an organization-assigned phone and must use your personal phone for work related texts, for your own protection, archive all messages on your personal phone that are work related.

For non-criminal infractions, an individual can be charged up to \$500 and reasonable attorney fees and costs. Most violations are inadvertent; for criminal sanctions, it must be knowing violation, which rarely occurs.

There are exceptions to Sunshine Law requirements regarding the communication between members and the body. You may go to lunch or see other Council members socially, as long as you do not discuss current Council related issues or issues that may come before Council.

Assistant General Counsel Robinson provided the citation for the recent opinion related to the Sunshine Law which came out of the 4th DCA on February 15, 2023: 2023 WL 2027556. She also mentioned the reference materials related to the ethics guidelines that were included in the Council's meeting packet.

No questions were asked by the Council members.

ITEM 2
Federal Funding Update
Bureau Chief Jennifer Miller
Florida Department of Law Enforcement
Information and Discussion

Chair Prendergast recognized Chief Jennifer Miller who provided an update on CJIS federal funding. Chief Miller stated since the last meeting, FDLE applied for NCHIP supplemental funding, and if awarded, the \$2.4 million grant would fund the purchase of 110 LiveScan devices for the local agencies. FDLE reviewed the total LiveScan devices replaced during the previous replacement process, in addition to the list of currently expiring devices from the vendors. FDLE should know in early summer if we are awarded these funds.

FDLE is continuing the spending on existing federal grants (NCHIP and NARIP) that fund the Multi Biometric Information Solution (MBIS) Modernization, Computerized Criminal History (CCH) Modifications, conducting research on missing arrest information, firearm transactions, and mental health records. FDLE does not anticipate applying for any additional new funding at this time.

FDLE also submitted a legislative budget request (LBR) for \$1.1 million to upgrade at least one latent print workstation in each county that currently has a latent workstation. The upgrade will offer those agencies the ability to continue to submit latent print data to FDLE following the completion of identified milestones in Phase 2 of the MBIS modernization. Additionally, the LBR included a request for the budget authority FDLE needs to spend the awarded grant funds to cover network increases and operations and maintenance for MBIS.

No questions were asked by the Council members.

ITEM 3
Multi Biometric Identification Solution (MBIS) Update
Senior Management Analyst Supervisor Josh Gray
Florida Department of Law Enforcement
Information and Discussion

Chair Prendergast recognized Senior Management Analyst Supervisor (SMAS) Josh Gray who provided an update on MBIS. SMAS Gray stated FDLE entered into a contract on October 28, 2022 to modernize FDLE's Biometric Identification Solution (BIS) system – a cloud-based platform providing faster and more accurate fingerprint searches. The project is proceeding as a two-phased approach. Phase 1a, which moves a copy of the current database to the cloud for disaster-recovery, began December 2022. Requirements gathering for Phase 1b, which moves the Rapid ID functionality to the cloud, was completed in February 2023. Phase 2 of the project will move all latent and tenprint processing to the cloud, as well as the addition of some new functionalities.

The tentative contract schedule includes Phase 1a implementation in the fall of 2023, followed by Phase 1b implementation in the spring of 2024. Phase 2 is scheduled for implementation at the end of 2024.

Crime Information Bureau (CIB) Biometric Services Section (BSS) staff members continue to provide ongoing updates to FDLE's local agency partners regarding this project. BSS has reached out to each individual booking agency, as well as all local latent users, to ensure FDLE maintains open lines of communication regarding current project statuses. BSS has also requested input from all local agencies on what types of improvements and changes the agencies would like to see in the modernized system.

BSS continues to utilize a mailing list to send out regular updates as the project moves forward. Those who would like more information on how to subscribe to the mailing list, or more information on the project itself, can email our Biometric Services Section at CJISBiometrics@fdle.state.fl.us.

No questions were asked by the Council members.

ITEM 4
Data Sharing Projects Update: Criminal Justice Data Transparency (CJDT), Uniform Arrest Affidavit (UAA)/Florida Arrest Affidavit (FAA), Uniform Crime Report (UCR) and Use of Force (UoF)
Bureau Chief Phillip Suber
Florida Department of Law Enforcement
Information and Discussion

Chair Prendergast recognized Chief Phillip Suber who provided an update on the different data sharing initiatives. Chief Suber began his update with UCR's statewide transition from summary-based to incident-based crime reporting. Since the last meeting, FDLE has introduced incident-based data to our crime data web page. This includes data for agencies that have submitted 2021 and now, 2022 FIBRS data. FDLE continues to review this data and make improvements in how this information is displayed on our public web page. As FDLE consumes more data from agencies, we expand our ability to display data and deliver a broader message of crime in Florida.

As of this week, 93 law enforcement agencies have completed the FIBRS testing process and been given permissions to submit the new data. This is an increase of 30 agencies since our last meeting in November. These 93 agencies represent over 48% of Florida's population and include 34 sheriffs' offices and 59 police departments. Another 73 agencies are actively working toward their transition.

As of last week, 59 local law enforcement agencies have submitted over a half million incidents through FIBRS since going online. For calendar year 2022, FDLE passed over 244,000 incidents on to the FBI's national repository.

For agencies that have not yet transitioned, FDLE is still collecting their summary-based data. For 2022, FDLE received data from 155 agencies. The 2022 summary-based data collection just ended, and FDLE will begin to analyze this information. 2022 will be the first year participation will be mostly split between the two varieties, and for this reason, FDLE will begin exploring methods to blend the two collections for one statewide report.

In July 2022, Law Enforcement UoF reporting became required by statute, and so far, 293 agencies participated in this effort. Agencies are required to report an incident that involves severe bodily injury, discharge of a firearm, or death of a subject. In the absence of a UoF event, the agency shall submit a "zero report" to affirm that nothing occurred that month. Since FDLE opened use of force reporting in 2020, which was voluntary at the time, FDLE has collected 5,047 zero reports and 411 incidents.

FDLE continues to look at ways to improve UoF reporting. Approximately 120 agencies still need to participate. FDLE is working to build consistency in monthly reporting for agencies, so no months are missing. Chief Suber stated agencies must remember the two-step process for submissions. These steps include the entry of the data, and then the verification by the Chief Executive (or designee). This process is identical to the submission of incident-based crime data.

The UAA is ready for agency adoption. Currently, just over 30 agencies are actively testing UAA submissions and preparing to move forward to the next step. One agency has opted to use the Florida Arrest Affidavit web application to comply with this requirement.

Since the November 2022 meeting, FDLE has continued onboarding CJDT contributors. The Clerks of Court, Public Defenders, Florida Department of Corrections, and Justice Administrative Commission are fully onboard and continuing with their submissions, and the Regional Conflict Counsel (RCC) is nearing full participation. The final three RCC districts are wrapping up testing and should be submitting data soon.

The State Attorney's Offices are one of our CJDT "dual submitters," and they must provide an Administrative report and a Case report. In December 2022, all 20 circuits had completed their Admin report submissions, and 13 circuits have submitted Case data.

County Detention Facilities also have two reports to submit: Admin and Booking or Arrest. 34 jails have completed the Admin requirement, and 27 have finished the Arrest submissions. FDLE is working closely with the jails to move them toward completion and to include the offer of financial assistance in the form of pass through funds.

Overall, FDLE has been very involved with assisting agencies navigate the process of getting started, submitting test data, refining errors, and moving into production. Additionally, we are working hard with our IT Project staff and vendor to ensure the various systems are running effectively.

Unfortunately, as with any new system, or in this case, multiple systems, and as more contributors on board, more varieties and volumes of data uncover needed improvements. Our partners are assisting us identify these data anomalies, and FDLE appreciates our partners' patience as we put fixes into place.

No questions were asked by the Council members.

ITEM 5
FBI CJIS Security Policy Update
CJIS Information Security Officer Chris Eaton
Florida Department of Law Enforcement
Information and Discussion

Chair Prendergast recognized FDLE CJIS Information Security Officer (ISO) Chris Eaton who provided high level overview of the updates to the FBI CJIS Security Policy modernization. ISO Eaton began by giving a brief history of the FBI CJIS Security Policy, including the current modernization efforts which began in 2020. The main driver in the modernization effort was the realization the technology is outpacing what is in current policy. There were also questions about the personnel security requirements, especially concerning cloud vendors and how the personnel screening applies. The CJISSECPOL Modernization Kickoff formally began in September 2020.

ISO Eaton provided a summary of the changes in CJISSECPOL 5.9.1.

- Policy Area 5.8: Media Protection (MP) – Modernized requirements for media policy and procedures, access, marking, storage, transport, sanitization and use
- Policy Area 5.12: Personnel Security – Provided clarification on screening requirements
- Appendix G.3 Cloud Computing – Provided clarification on requirements

ISO Eaton also provided a summary of changes in CJISSECPOL 5.9.2. He noted three control families were modernized in version 5.9.2, including Awareness and Training (AT), Identification and Authentication (IA), and System and Information Integrity (SI). SA-22 was also updated, and it was considered a fast track item. SA-22 relates to unsupported system components when there is no longer support from the developer, vendor, or manufacturer.

Awareness and Training (AT) Control Family

There are four controls in the Awareness and Training (AT) control group/family, and it is considered a complete section replacement for the former Security and Awareness Training Policy area. The new requirements are considered auditable/sanctionable by the FBI beginning October 2023.

AT-1 Policy and Procedures

Agencies are required to have a training policy. The policy must be reviewed and updated annually. The policy must also be updated if there are: changes in the information system operating environment; security incidents; and changes to CJISSECPOL. FDLE will provide sample policy language for agencies to start from and tailor to their agency.

AT-2 Literacy Training and Awareness

AT-2 is a new requirement for agencies. Agencies are required to provide training prior to accessing CJI and annually thereafter. Training must also be provided any time there are system changes or within 30 days of a security event. Training topics must include insider threat, social engineering and mining, and training on processing personally identifiable information (PII). Additionally, agencies must employ one or more of the following techniques to increase security awareness:

- Display posters
- Supplies inscribed with security and privacy reminders
- Logon screen messages
- Email advisories
- Awareness events

FDLE is creating sample training that will help agencies meet this requirement. Agencies can use this training if they wish and tailor it for specific agency needs. FDLE will also have different items that agencies can use or post at their agency to meet the requirement for displaying media.

AT-3 Role Based Training

AT-3 is primarily handled by our vendor CJIS Online and nexTEST. The previous levels 1-4 training are being replaced by role-based training, and the new training will be required before accessing a CJIS system, and annually thereafter. Previously, the training was required within six months of hire and required every two years. As a result of the annual training requirement, Limited and Full Access training will now be required annually, and it will contain all of the requirements to meet the security awareness requirements. Both CJIS Online and FDLE are working to update the curriculum to meet this requirement, which becomes auditable and sanctionable October 2023

AT-4 Training Records

Individual training records are required to be maintained for three years. This requirement accounts for the typical three-year audit cycle.

Identification and Authentication (IA) Control Family

IA was a strike all and replace in policy, and it expanded from 12 pages to over 80 pages of requirements. FDLE is working to understand the requirements. Multi-Factor Authentication (MFA) will be required for agencies, and it does not matter who you are or where you are, MFA will be required. MFA applies for privileged and non-privileged accounts, and it can occur at the network level or the application level. The requirements are complicated with each type of authenticator having a specific set of requirements. FDLE is working to understand the requirements, so we can help agencies comply.

When the Data Categorization task force met to look at how CJI should be categorized and protected, the task force decided to categorize CJI as moderate. Using NIST standards, the risk profile for moderate is Authenticator Assurance Level 2 (or AAL2). AAL2 requires the following MFA authenticators be used:

- Multi-Factor One Time Password (OTP) Device
- Multi-Factor Cryptographic Software and
- Multi-Factor Cryptographic Device

There are also specific requirements for biometrics. If using biometrics, they can only be used as a part of MFA with a physical authenticator. This is separate from unlocking a device or device authentication.

When implementing AAL2 and a memorized secret, formerly known as password, the other authenticator must be a possession based (or something you have) authenticator from the following:

- Look-Up Secret
- Out-of-Band Device
- Single-Factor OTP Device
- Single-Factor Cryptographic Software
- Single-Factor Cryptographic Device

There are also identity proofing requirements. These are new requirements for verifying the identity of someone requesting access to a CJIS system. FDLE is working through those requirements.

Agencies have until October 2024 to comply with these new requirements. This gives FDLE some time to study these requirements and give proper guidance to agencies. It is possible some of these requirements will change some before the final version 6.0 is released. Currently, FDLE is educating agencies on the new requirements; educating ourselves on the requirements; and seeking guidance from the FBI.

System and Integrity (SI) Control Family

SI is the last of the Control Group updates, and this area requires agencies to manage risks from system flaws/vulnerabilities through the establishment of an effective system and information integrity program. This includes requirements for:

- System monitoring
- Security alerts, advisories and directives
- Software, firmware, and information integrity
- Spam protection
- Information input validation
- Error handling
- Information management and retention/information disposal
- Memory protection
- File integrity
- Includes timelines for flaw remediation

This change is auditable/sanctionable by October 1, 2023.

System and Services Acquisition (SA) – Fast Tracked Item

SA-22 covers unsupported system components, and it requires organizations to replace components when they are no longer supported. Unsupported components can result in a security vulnerability to an agency's information system. The item will be part of the SA control family once it is modernized. With unsupported systems being such a security risk and one of the leading ways cyber criminals attack a network, SA-22 was deemed important and fast tracked. This requirement will be auditable and sanctionable by the FBI on October 1, 2023.

Future updates

ISO Eaton provided information on future updates. Three more control groups were approved in December 2022. Those control groups are Access Control (AC), Incident Response (IR) and Maintenance (MA). All three groups were approved by the Advisory and Policy Board (APB) in December 2022 with an expected spring 2023 publish date for CJISSECPOL v.5.9.3.

In spring 2023, the APB will review for approval six more control groups: Planning (PL), Physical and Environmental Protection (PE), Contingency Planning (CP), Audit and Accountability (AU), System and Communications Protection (SC), Risk Assessment (RA) Control Groups.

There is also a topic paper on direct/indirect access to CJI, which could reduce the requirements on CJI that is considered indirect. If the topic paper is approved, they would have to go back and revisit the groups already approved.

The APB's goal is to review and approve the remaining areas and control groups in 2023 with a complete review for full modernized policy version 6.0 in spring 2024.

Questions from the Council:

- Council Member Sawyer: Will there be possible remediation funding opportunities available for agencies for to meet the remediation needed for the system enhancements?
 - ISO Eaton stated there is funding through Florida Digital Services (FDS). The FDS application closes this week.
- Council Member Sawyer: Council Member Sawyer stated he will follow up with FDS, and he asked if the funding is more on the cybersecurity side.
 - ISO Eaton responded the discussions he has had with FDS indicated cybersecurity may be tied to the funding.
- Council Member Timmann: The Clerks received FDS funding. With FDLE's knowledge of how labor intensive this task is, would FDLE be open to holding a Teams meeting or webinar with the Clerks regarding the dates and requirements prior to the next round of audits?

- ISO Eaton indicated it part of FDLE's outreach is to discuss with agencies the requirements and help educate them of the upcoming changes and deadlines. FDLE will work with the Clerks to establish a meeting, if requested.

ITEM 6
2023 CJIS Annual Training Symposium
Information Item

Chair Prendergast asked Council members to review the information sheet included in the agenda packet regarding the 2023 CJIS Annual Training Symposium to be held on September 26-28 at the Signia by Hilton Orlando Bonnet Creek.

CLOSING REMARKS

Chair Prendergast shared the following regularly scheduled meeting dates:

- Monday, September 25, 2023 from 1:00 p.m. – 3:00 p.m. co-located at the CJIS Annual Training Symposium venue at the Signia by Hilton Orlando Bonnet Creek;
- Tuesday, March 26, 2024 at 9:30 a.m. EDT – virtual only meeting; and
- Monday, October 21, 2024 – Co-located at the 2024 CJIS Annual Symposium venue at the Hilton Daytona Beach Oceanfront Resort (time to be determined).

Chair Prendergast asked for a motion to adjourn. Council Member Sawyer moved to adjourn the meeting, and Council Member Broadway seconded. The meeting was adjourned at 10:18 a.m.