

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

**MINUTES OF MEETING
Wednesday November 13, 2024
Video Conference**

Members Present:

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

Charles Broadway, Chief, Clermont Police Department

Donald Edenfield, Sheriff, Jackson County Sheriff's Office

Mike Prendergast, Sheriff, Citrus County Sheriff's Office

Edward Hudak, Jr., Coral Gables Police Department

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

Spencer Hathaway for R.J Larizza, State Attorney, 7th Judicial Circuit

Ryan Schenck, Designee for David A. Wyant, Chair, Florida Commission on Offender Review (COR)

Carolyn Timmann, Martin County Clerk of Circuit Court and Comptroller

David James, Designee for Secretary Ricky D. Dixon, Department of Corrections (DC)

Doug Smith, Designee for Attorney General Ashley Moody

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

Olu Oyewole, Designee for Secretary Eric S. Hall, Department of Juvenile Justice (DJJ)

Major Amanda Meyer, Designee for Director Dave Kerner, Department of Highway Safety and Motor Vehicles (DHSMV)

Members Absent:

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

WELCOME MEMBERS and OPENING

Chair Sawyer called the meeting to order at 9:30 a.m. and introduced new member Ryan Schenck, representing the Florida Commission on Offender Review, to the CJJIS Council. Council Member Schenck thanked members for the opportunity to serve on the Council and looks forward to working with the Council members.

Approval of the July 10, 2024 CJJIS Council Meeting Minutes

Chair Sawyer requested a motion to approve the July 10, 2024 CJJIS Council meeting minutes. Council Member Hudak moved, and Council Member Prendergast seconded the motion to approve the July 10, 2024 minutes. The motion passed.

ITEM 1

Multi Biometric Identification System (MBIS) Update

Bureau Chief Mary Jackson

Florida Department of Law Enforcement

Information and Discussion

Chair Sawyer recognized Chief Jackson who provided an update on MBIS. 109 livescan devices paid by grant funds were delivered to local agencies. Latent devices are currently being delivered to sheriff offices and police departments that have latent stations. FDLE is in the testing phase with the vendor. The Department of Corrections (DC) and another agency is interested in piloting an iris program. Shortly after MBIS is live, FDLE will begin onboarding these agencies for the iris program.

No questions were asked by the Council members.

ITEM 2

Automatic Sealing of Criminal History Records and Making Confidential and Exempt Related Court Records Update

Bureau Chief Mary Jackson

Florida Department of Law Enforcement

Information and Discussion

Chair Sawyer recognized Chief Jackson who provided an update on the automatic sealing of criminal history records and making confidential and exempt related court records. FDLE and the Florida Clerks and Comptrollers (FCCC) continue to work together on implementation the provision of SB 376, the automatic sealing of criminal history records. FDLE is working with the clerks on errors as they arise and will address the issue with case numbers spanning multiple cycles once MBIS goes live.

The following comments were made at the end of the discussion:

- Council Member Timmann: Thanked her clerk of court partners, and FDLE, for working with the clerks to fully implement this change. Council Member Timmann stated the clerks will continue to work through the issues to meet the requirements.
- Chair Sawyer: Thanked all those involved in working together.

ITEM 3
Uniform Statute Table
Bureau Chief Mary Jackson
Florida Department of Law Enforcement
Information and Discussion

Chair Sawyer recognized Chief Jackson who briefed the Council on the Uniform Statute Table. The updated statute table went into production on August 13, 2024. FDLE continues to address items raised by the Uniform Statute Table Workgroup, including citing offenses at the element instead of the penalty phase and moving from “catch all” Arrest Offense Numeric (AON). The drug statute chapter 893 review is complete, and the changes were made with the Spring cleanup deployment.

The following comments were made at the end of the discussion:

- Chair Sawyer: During a demonstration on the DC digital scoresheet, a question was if DC is considering using the uniform statute table.
 - FDLE is not aware if DC plans to utilize the uniform statute table as part of their digital scoresheet.

ITEM 4
Federal Bureau of Investigation (FBI) Audit
CJIS Information Security Officer (ISO) Chris Eaton
Florida Department of Law Enforcement
Information and Discussion

Chair Sawyer recognized FDLE CJIS Information Security Officer (ISO) Chris Eaton who provided update on the upcoming FBI audit. The FBI CJIS Division conducts audits, once every three (3) years of each CJIS Systems Agency, to assess agency compliance with applicable statutes, regulations, and policies. The audit includes a sample of criminal justice agencies and non-criminal justice agencies. Florida is scheduled to be audited February 10-14, 2025. FDLE received pre-audit questionnaires for all the different areas which includes an audit of FDLE, and a mix of local agency audits. Audits will be conducted remotely, and some will be on site.

Types of audits include:

- Use of Force
- National Incident Based Reporting System (NIBRS)
- National Sex Offender Registry System (NSOR)
- National Crime Information Center (NCIC)
- National Instant Criminal Background Check System (NICS)
- Information Technology Security (ITS)
- Next Generation Identification service (NGI)
- National Data Exchange system (NDex)

FDLE audit staff will assist local agencies that are selected by performing a preaudit to identify any potential issues in advance, and FDLE staff will be present with the agency when the FBI visits.

No questions were asked by the Council members.

ITEM 5
Bipartisan Safer Communities Act Update
Bureau Chief Tracy Townsend
Florida Department of Law Enforcement
Information and Discussion

Chair Sawyer recognized Chief Townsend who provided an update on the Bipartisan Safer Communities Act (BSCA) regarding individuals who are under the age of 21 seeking to purchase a long gun, and the Federal Bureau of Investigation's (FBI) NCIC Stolen Gun file.

FDLE's Firearm Eligibility Bureau (FEB) is comprised of 2 sections. The Firearm Purchase Program (FPP) and the Eligibility Research Unit (ERU).

The FPP is responsible for conducting background checks for individuals who wish to purchase a firearm in Florida, while the FBI handles this process for most of the other states. At the time of the firearm background check, the individual's demographics are compared to records in state and federal databases which include Florida Crime Information Center (FCIC), NCIC, the Interstate Identification Index (III), and NICS.

The ERU is tasked with conducting firearm research to help determine an individual's eligibility due to missing information in their criminal record, such as missing dispositions, charge level, and final determinations for probations. The unit is also responsible for firearm appeals, and the Florida Mental Competency application (MECOM).

The FDLE acts as a Point of Contact (POC) State with the FBI. As a POC, FDLE becomes an extension of the FBI and is required to adhere to their policies and federal law as well state of Florida policies and procedures.

On June 25, 2022, the BSCA was signed into law. The Act expanded the firearm background check for individuals under 21 who were seeking to purchase a long gun. The provisions outlined in the Act seek to close any gaps in juvenile criminal and/or mental health information that may not already be available when a NICS background check is conducted for a firearm.

The Act set the following requirements for FDLE and the FBI.

1. To perform the expanded background check within 3 days.
2. To contact the state's criminal history repository, juvenile justice information system, and custodian of mental health adjudication records.
3. Contact local law enforcement in the jurisdiction in which the person resides to see if they have any additional information on the individual.

FDLE is the repository for criminal history information and mental health records, and we have direct access to the DJJ for our juvenile research which makes it easier to meet this requirement of the Act.

In Florida, individuals under the age of 21 may only purchase a long gun if they are a law enforcement officer, a correctional officer, or a servicemember per Florida Statute 790.065. This narrows the population that will require the expanded background check. This “exception” was put into place due to the Marjory Stoneman Douglas Act in 2018. The ability to purchase a handgun is still federally restricted until the individual’s 21st birthday.

In 2023, FEB processed 515 under 21 requests with only two receiving a non-approval.

Section 12004 of the BSCA gives Federal Firearm Licensees (FFLs) access to certain law enforcement data, for the purpose of stopping the illegal trafficking of firearms, by giving FFLs access to the information in the FBI’s NCIC Stolen Gun File. Currently, the only option available for the FFLs to conduct a search of the FBI’s NCIC Stolen Gun File is to partner with their local law enforcement agency. Based on the new rule, law enforcement may assist the FFLs with the NCIC stolen gun queries.

FDLE is working with the FBI to make this information available to the FFLs through the Florida Eligibility System (FES), which is used to conduct criminal history record checks for individuals who want to purchase or transfer a firearm in Florida. The release of the NCIC Stolen Gun File dashboard in FES is tentatively set for November 2024. Once this information is available in FES, FDLE will notify law enforcement.

No questions were asked by the Council members.

ITEM 6

CJJIS Council Workplan – Automated License Plate Reader Guidelines and Strategic Plan

Chief Edward Hudak, Jr.
Coral Gables Police Department

Action Item

Chair Sawyer recognized Council Member Hudak who provided an update on the Automated License Plate Reader (ALPR) Guidelines. The proposed changes are based on recommendations from subject matter experts on the FBI’s CJIS Security Policy (CJISSECPOL). ALPR systems that utilize an extract of ALPR data or perform secondary queries of state and national systems that access personal identifiable information or criminal justice information shall conform to the CJISSECPOL.

- **Action Item: Chair Sawyer asked for a motion to adopt the revisions to the ALPR Guidelines. Council Member Timmann made the motion to adopt the ALPR Guidelines. The motion was seconded by Council Member Broadway. The motion passed.**

During the workgroup's discussion of the Council's workplan and strategic plan, the conversation focused on the timeframe of the Council's strategic plan, the flow of information, and frequently changing technology (i.e. artificial intelligence).

The strategic plan includes the Council's Directions and Council Member Hudak asked if Council members can take the Directions into account when reviewing the strategic plan. Council members were asked to review the strategic plan and provide feedback to FDLE staff.

The following comments were made at the end of the discussion:

Chair Sawyer: The goals in the current strategic plan are still relevant and can serve as guiding principles as we update the plan. Should a workgroup review the recommendations prior to the February 18, 2025 Council meeting?

Council Member Hudak: The workgroup currently in place to review the strategic plan can meet to review the proposed changes.

- **Action Item: Council members to review the Council's Strategic Plan and provide feedback to Brenda Boyd and Rachel Truxell by December 31, 2024. FDLE staff will compile the responses for the workgroup to review, and the Council members to discuss during the February 18, 2025 meeting.**

ITEM 7

FBI CJIS Security Policy Update

CJIS Information Security Officer (ISO) Chris Eaton

Florida Department of Law Enforcement

Information and Discussion

Chair Sawyer recognized FDLE CJIS Information Security Officer (ISO) Chris Eaton who provided updates to the FBI CJIS Security Policy (CJISSECPOL) v. 5.9.5 which was published in July 2024.

Changes in v. 5.9.5 include:

- Direction given for priority and implementation deadlines, how the FBI implements the new policies and in what order.
- The sunset of basic password standards. As of September 30, 2024, multi-factor authentication is required when accessing criminal justice information.
- Modernized Configuration Management control family.

All control families have gone through the FBI Advisory Policy Board (ABP) process. The following control families have been published:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Configuration Management (CM)

- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental (PE)
- Planning (PL)
- Risk Assessment (RA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Assessment, Authorization, & Monitoring (CA), Personal Security (PS), System & Services Acquisition (SA), and Supply Chain Risk Management (SR) have been approved by the APB, but not published.

As the security controls in the CJISSECPOL are modernized, agencies have been unclear on which controls should be implemented in a particular order. Previously, modernized security controls were assigned deadlines for auditability based on the release date of the version they first appear in the CJISSECPOL and how that date falls relative to the FBI CJIS Audit Unit's (CAU) audit schedule which begins on October 1 of each fiscal year.

The FBI researched the Adversarial Tactics, Techniques, and Common Knowledge, or MITRE ATT&CK, which is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Using MITRE ATT&CK data and cross-mapping it to the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 Rev. 5.1, Security and Privacy Controls for Information Systems and Organizations, moderate security controls, the following priorities for implementation were developed:

Existing – Existing CJISSECPOL requirements that are currently auditable.

Priority 1 (P1) – Priority 1 controls are determined to be the most critical and will be auditable starting on October 1, 2024. Analysis shows that these controls considerably improve your security posture against known active attacks.

Priority 2 (P2) – Priority 4 (P4) – Priority 2, Priority 3, and Priority 4 will fall into a zero-cycle audit status. The zero-cycle began October 1, 2024, and ends September 30, 2027.

Each modernized control is marked with one of the above priorities. Non-modernized sections do not have markings but are considered “existing” requirements and continue to be auditable.

The zero-cycle audit controls encompass all new modernized controls not previously in the CJISSECPOL and not identified as being Priority 1 [P1]. The zero-cycle controls account for roughly 56 percent of all controls which will significantly reduce the initial burden on agencies while allowing time to enhance security posture. These controls will be auditable after the zero-cycle audit period above has lapsed.

Agencies can further use the recommended priority code designation associated with each security control to assist in making decisions for control implementation. A Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control; a Priority Code 3 [P3] control has a higher priority for implementation than a Priority Code 4 [P4] control. This recommended prioritization sequencing helps ensure that security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources.

The Configuration Management (CM) family of controls establishes requirements like those previously in Section 5.7 of the CJISSECPOL. Many of the existing requirements were carried over. However, there are new controls which address aspects of managing the configuration of the information system not previously considered in the CJISSECPOL. The updated control family includes new controls for creating a system baseline configuration, maintaining previous versions of baseline configurations to support rollback, establishing a configuration change process, and maintaining a system component inventory.

CM changes consist of:

CM-2 Baseline Configuration

CM-2 Baseline Configuration requires agencies, in addition to having a complete topological drawing, to also have a baseline configuration. Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Baseline configurations of systems reflect the current enterprise architecture. Appendix C of the CJISSECPOL includes sample topological/network diagrams.

CM-2 Baseline Configuration Control Enhancements

CM-2 Baseline Configuration Control Enhancements require the use of automated mechanisms, when possible, include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation. Issuing devices (mobile devices) with CJISSECPOL compliant configurations to individuals travelling to locations that the organization deems to be of significant risk and upon return from travel, examining the device for signs of physical tampering, and ensuring all security controls are in place and functional.

CM-3 is Configuration Change Control

CM-3 Configuration Change Control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and

unscheduled or unauthorized changes. Agencies must have a process for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes.

CM-8 is System Component Inventory

Agencies must develop and document an inventory of system components. System components include hardware, software, and firmware and inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols. Agencies must review and update their system component inventory annually.

In recent CJISSECPOL updates to the Council members have inquired on funding opportunities for implementing the provisions of the CJISSECPOL.

- Florida Digital Services has grant opportunities for local agencies.
- The Cybersecurity Infrastructure Security Agency (CISA) has state and local cybersecurity funding available.
<https://www.cisa.gov/state-and-local-cybersecurity-grant-program>
- Additionally, through the Bureau of Justice Statistics (BJS), there is National Criminal History Improvement Program (NCHIP) funding available. NCHIP funding is used primarily to improve the integrity and availability of state criminal history repositories. BJS has stated they are open to the idea of using grant funds for cybersecurity; however, we are not aware of a state that has applied for BJS funds for cybersecurity.
<https://bjs.ojp.gov/programs/national-criminal-history-improvement-program>

FDLE CJIS is holding county-wide CJIS compliance meetings. During these meetings, CJIS will offer the opportunity for an open discussion with criminal justice partners regarding the modernization of the FBI CJIS Security Policy and the effects of those requirements throughout the criminal justice community on a county-wide basis. This approach will allow the discussion to be centered around the local agencies to include each partner's CJIS network, shared resources, and vendor support in an effort to streamline requirements and reduce undue hardship on each agency.

Additional information on the county-wide CJIS compliance meetings will be provided through a CJIS memo in the upcoming weeks.

The following comment was made at the end of the discussion:

Chair Sawyer: Thanked ISO Eaton on providing information on the funding opportunities and the outreach through the county-wide CJIS compliance meetings.

ITEM 8
Speed Zone Cameras
Information Sheet

Chair Sawyer asked Council members to review the information sheet included in the agenda packet regarding the speed zone cameras. The following information was included on the information sheet:

In order to strengthen the enforcement and safety of school zones in Florida, HB 657 was signed into law by Governor DeSantis on May 31, 2023. The new law, which became effective July 1, 2023, authorizes counties and municipalities to enforce the school zone speed limit through the use of speed detection systems.

These systems typically employ a camera-equipped radar detection device to identify motorists that are driving 10mph or more over the posted school zone speed limit. In these instances, the camera captures a photo of the vehicles license plate, and the registered owner of the vehicle may receive a citation in the mail.

The use of school zone speed cameras is part of a broader effort to enhance the safety of children by reducing speeding in areas where they are likely to be present. The goal is to improve compliance with speed limits in school zones, reducing the likelihood of accidents involving children.

In order to obtain owner registration information for a vehicle that may have violated school zone speed limit, law enforcement agencies query motorist records from Florida Highway Safety and Motor Vehicle and out-of-state repositories through the use of the Florida Crime Information Center (FCIC), and/or the interstate justice and public safety network, Nlets. FDLE, as the CJIS Systems agency in Florida, plays a role in the on-boarding process for systems accessing FCIC and Nlets. Agencies are tasked with submitting detailed information about a new FCIC interface for review and approval before access is provided. This can include:

- Network diagrams for the agency and interface.
- Vendor screening information.
- Contracts, agreements, or memorandums of understanding.
- Other pertinent information about the interface that helps demonstrate FBI CJIS Security Policy compliance.

Since becoming law, there has been a large interest from counties and municipalities to take the necessary steps outlined in HB 657 to implement school zone speed detection systems. FDLE has received numerous requests from partnering law enforcement agencies to on-board school zone-related systems in recent months, and we anticipate that trend to continue.

Similar to other automated detection/enforcement initiatives, such as red-light cameras and license plate readers, school zone speed detection systems are another example where law enforcement is turning to technology to assist with enhancing public safety. As this initiative continues to expand, it may be beneficial for the CJJIS Council to assess whether

to provide additional best-practice guidelines for agencies seeking to employ these technologies to support their mission.

No questions were asked by the Council members.

ITEM 9
Data Sharing Update on Onboarding for CJDT and FIBRS
Information Sheet

Chair Sawyer asked Council members to review the information sheet included in the agenda packet regarding the onboarding of CJDT and FIBRS entities. The following information was included on the information sheet:

Submitting agencies are continuing to make progress for both Criminal Justice Data Transparency (CJDT) and Florida Incident-Based Reporting System (FIBRS). Staff works continuously over the phone, email, and through virtual meetings and in person meetings with agencies to resolve difficulties and bring them on board. For CJDT, the remaining agencies that are not submitting are some of the county detention facilities. [Nineteen](#) detention facilities remain to be compliant in either booking, administration, or in some cases both. As the year progresses, we expect significant progress toward completion. For FIBRS, 62% of the state of Florida's population is covered by agencies that are submitting in production. Among the remaining agencies not yet in production, 45% of those agencies are testing in preparation to go into production.

No questions were asked by the Council members.

ITEM 10
CJJIS Council Chair and Vice Chair Elections
Director Lucy Saunders
Florida Department of Law Enforcement
Action Item

Chair Sawyer recognized CJIS Director Lucy Saunders who thanked the current chair and vice chair of the Council. Section 943.06, F.S. requires the CJJIS Council to annually elect its chair and vice chair. Director Saunders opened the floor for nominations for the CJJIS Council Chair.

Council Member Hudak nominated Council Member Broadway for Chair and Council Member Timmann seconded the nomination. There were no other nominations. Council Member Broadway accepted the nomination and thanked Chair Sawyer for serving as chair this past year and for his leadership.

Director Saunders opened the floor for nominations for the Vice Chair. Council member Hudak nominated Council Member Timmann, and Council Member Broadway seconded

the nomination. There were no additional nominations. Council Member Timmann accepted the nomination.

Congratulations Chair Broadway and Vice Chair Timmann.

CLOSING REMARKS

Chair Sawyer shared the following regularly scheduled meeting dates:

- Tuesday, February 18, 2025 from 9:30 – noon: This will be a virtual meeting via Microsoft Teams.
- Monday, July 14, 2025 (Time to be determined) The meeting will be an in-person only meeting and will be co-located at the 2025 CJIS Annual Training Symposium venue at the Hilton Orlando.

Chair Sawyer asked for a motion to adjourn. Council Member Hudak moved to adjourn the meeting, and Council Member Broadway seconded. The meeting was adjourned at 10:25 a.m.