5/6/21 OSP Responses to questions for SB204A

Access to LEDS can be very involved due to the restrictions implemented by law. Clarification as to what records within LEDS a review body would need for this purpose may be helpful to ensure there is no misunderstanding as to what is/is not available within LEDS for such reviews.

To clarify, information such as police reports, police investigation documents, police certifications or credentials, witness information are not contained in LEDS. Due to the restrictions and confidentiality of criminal justice information (CJI), any data that relates to CJI that may be contained in these local police record types of documents is required under the FBI CJIS Security Policy to be removed or redacted should documents be made available for review.

The following responses are provided with the assumption that there are records within LEDS that would be applicable to or benefit the review process.

1. Who would provide authorization and oversight for body that gains access to LEDS?
   This is a question that OSP would ask for clarification as well.

   Municipality is broad and OSP would require the responsible agency/party to enter into agreement with OSP for issuance of access credentials and to outline all rules, policy, and procedures that must be followed regarding review board members, facility security, data access, storage and destruction, etc. Key persons within the authorized agency would be subject to the same background check requirements to maintain an authorized review board.

2. What type of oversight will there be?
   By OSP:

   - Entity must enter an access and use agree with OSP for compliance of all policies pertaining to CJIS data access and security.
   - All parties designated for access must pass a fingerprint-based background check.
   - All parties must be trained for the level of access and recertified every 2 years.
   - Audit conducted minimally every 3 years at the state level.

   By FBI: In addition to state requirements - Triennial audit to include review of records accessed, how used, maintained, destroyed as required. Requires agency to immediately self-report any breach or potential breach of data security, loss of records, etc.

3. How would OSP maintain integrity of the system and system access.
   - Through audit and compliance of CJIS Security Policy.
   - Written agency agreement that all policy, rules, and security requirements will be followed.
   - Hold agency accountable to comply with all policy requirements for data safety.
   - Entity is responsible to ensure all authorized users have passed the CJIS Security fingerprint-based background check. Applicant fingerprints will be retained for continuous

evaluation for each user with access until such time as the agency/entity reports to OSP the applicant is no longer required to have access.

- Entity must assign a LEDS Representative and LASO that are responsible to ensure appropriate use and access within the agency/entity. These representatives are required to maintain LEDS training and security clearance.
- All users must pass access-appropriate trainings and remain current.
- Conduct agency audit for use and access minimally every 3 years.
- If direct logical (computer) access is intended, all authorized users must be trained, pass and maintain certification levels.
- IT infrastructure review and audit are required. Any contractors with access to CJI through an entity/agency operation must be backgrounded, trained, and follow all security requirements.

4. Access for CJIS, if you have criminal background, you are denied access.
   If a person does not pass the CJIS Security background check, they cannot be allowed access to CJI. Not all criminal events will be disqualified.

5. Citizen advisory committees may want someone with lived experience. How would this play out if they can't pass the CJIS clearance?
   If a member is determined ineligible, they cannot have access to CJI.

6. How do they ensure that folks who are not supposed to have access won't have access?
   Entities that have been authorized access to LEDS have the responsibility to comply with all CJIS Security Policy, rules, and requirements.

   CJIS records are confidential and limited by statute for both criminal justice and non-criminal justice purposes. One of the key safeguards for access security is a nationwide fingerprint background check. However, OSP would not be authorized to conduct such a check for the purposes of SB204A, and review board backgrounds would likely be limited to within Oregon only.

   A legislative or executive designation of "criminal justice agency" for an entity that does not operate by definition as performing the "administration of criminal justice" would not be sufficient to authorize OSP to conduct a nationwide background check through the FBI as required by the CJIS Security Policy. To gain authority to conduct a nationwide background check for non-criminal justice purposes would require specific statutory language to meet FBI requirements to be approved by the US Attorney General. The same process would be required as for other oversight agencies, such as the Board of Nursing, Office of Child Care, Department of Public Safety Standards and Training. If authority and approval were obtained through FBI, all applicable background check fees would apply for each responsible oversight body and each review board applicant background check.

   [Administration of criminal justice means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.]

7. How can they ensure data security and prevention of wrongful dissemination?
   The responsibility for all review board members falls to the entity given the oversight of review boards. The entity again, would commit by agreement with OSP that they will comply with all requirements to ensure the security of the data and maintain confidentiality and record integrity.

   The entity must agree to a secured facility and environment where records may be accessed and to the immediate destruction of any records no longer in use.

8. Under SB 204, it sounds like "civilian" oversight agencies already exists and this bill would give them access to LEDS, because they were unable to perform their oversight this summer in Portland without it. But all the testimony in SB 621 indicated that Portland was unable to set up a "community" oversight board that the voters approved. Are "civilian" and "community" boards different? I am curious about the definition of "civilian oversight agency or review body."
   OSP cannot answer these questions.

9. How many bodies will get access to LEDS with this bill? It seems broad. What other bodies might get access?
   OSP agrees, this definition is broad, and this is a question that OSP would wish to gain clarification as well. The larger the scope, number of individuals involved and movement of participants, the higher the impact on OSP resources needed to manage activity, access, and security.

   For any bodies that are given authority for access to criminal justice records, the same requirements must be applied and monitored for each authorized body, each review board member initially and ongoing throughout the duration of their participation. If a member is no longer a participant, the oversight body must immediately notify OSP to remove all access and destroy the members CJIS Security fingerprint card to ensure compliance and mitigate any unauthorized access by the entity for activity that could occur after a member is no longer in their role.

10. What is the plan for allowing expanded access to LEDS while maintaining the integrity of the system against improper access and use of the data? Terminal security, building security, individual access, etc.
    All these items are subject to and addressed under the CJIS Security Policy and fall first to the entity being authorized under the legislation. It is the responsibly of the authorized entity/agency to agree to and comply with all requirements. OSP CJIS Division and audit staff would be responsible to ensure accountability and compliance is maintained by all authorized parties.

11. What federal restrictions will there be on the type of information accessed through the LEDS system?

While SB204A designates a new category of "criminal justice agency", due to the federal definition of the Administration of Criminal Justice, OSP anticipates that access to CJI for this purpose will not be authorized by FBI and therefore access would be limited to Oregon information only, including the fingerprint-based background check on entity staff and review board members. Any access to federal criminal offender record information for a non-criminal justice purpose is restricted and requires specific authorization and access only fingerprint-based check.

12. What specific information will accessible through LEDS?

Records contained in LEDS are confidential and access is restricted for criminal justice purposes and when authorized, for limited non-criminal justice purposes. Examples of the records contained in LEDS are:

- **Computerized Criminal History (CCH)** – CCH is a formal record of arrest, prosecution, court case outcomes, and custodial status for persons associated with crimes committed in the state of Oregon. This information is commonly reported in the form of record of arrest and prosecution "RAP sheets".
- **Hot Files** – Hot files are formal records, or data stores, associated with types of common information, typically including, but not limited to, Vehicles, Guns, Persons, and Articles. Hot files are a generic term traditionally derived from the term stolen, but it has a contemporary meaning beyond that of simply stolen items (e.g., missing persons).

13. What training will be required to access the system?

- All users must pass access-appropriate trainings and remain current.
- If direct logical (computer) access is intended, all authorized users must be trained, pass and maintain a LEDS certification at the appropriate access level.
- Any contractors with access to CJI through an entity/agency system must be Security Awareness trained and follow all security requirements.

14. What certification standards, if any, will be required?

Anyone authorized for access to CJI must go through the access-level appropriate training and certification. Recertification is required for each level.

15. Please explain the audit requirements that will be required in expanding access and the procedure for revocation of LEDS access.

The authorized entities will be required to be audited for both Access and Use and Information Technology (when applicable). Audit requirements are for both the state (OSP) and federal (FBI) level to ensure data integrity is maintained. All audit activity is covered under the CJIS Security Policy. Entities are responsible to address and answer in writing all findings and satisfactorily correct any issues of misuse, breach, training, and data security to maintain access for the entity.