Criminal Justice Background Check Playbook: An Industry Best Practices Guide

MARCH 2020

Authors

IJIS Institute's
CJIS Advisory
Committee's
Background Check
Working Group

IJIS Institute

Acknowledgments

This document is a product of the IJIS Institute, which is a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity.

We would like to extend a special thanks to the FiveBy and Microsoft CJIS team for their help in writing this playbook:

Cynthia Bakken
Minh Bui
Danielle Knight
Jason Nguyen

IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

CJIS Advisory Committee

Background Check Working Group

Comments and Questions

Your comments and questions are welcome! Please contact the IJIS Institute at info@ijis.org or 1-703-726-3697.

Table of Contents

1 | CJIS Overview

Founded in 1992, the Criminal Justice Information Services (CJIS) is the largest branch of the Federal Bureau of Investigation (FBI), where it houses biometric, identity history, biographical, proprietary, and case/incident historical data. Since then, the need to store and securely transport sensitive data has increased as more data becomes available, whether through legal or illegal activities.

CJIS information is accessed through online and offline resources as local, state, federal, and tribal governments migrate data to cloud providers. Therefore, companies and cloud providers share a responsibility to protect all data when stored and while in the cloud.

As a result of increased data, the FBI released several standards to ensure the confidentiality and security of Criminal Justice Information (CJI). This playbook provides best practices for managing users who request CJI access, as well as the required state-level background checks to access CJI. This playbook also addresses best practices to use when managing background checks for personnel who require any CJI access.

2 | About the CJIS Playbook

The FiveBy Solutions - Microsoft CJIS Operations team, who are members of the Integrated Justice Information Systems (IJIS) Background Check Working Group, developed this playbook to help staff from member companies with developing policies and procedures for compliance among local, state, federal, and tribal governments with CJIS access.

This playbook recommends the best practices listed below to achieve success, which can apply to small- and large-scale operations. They provide efficiency when initiating, operating, maintaining, and increasing the bandwidth of your company's CJIS organization.

- The most important component when vetting personnel for a CJIS data environmental clearance is to follow the FBI CJIS security policy.
- All data must be handled in a professional and organized manner to ensure the safety of personnel and their Personally Identifiable Information (PII).
- Each section detailed in the CJIS Playbook should be reviewed. All are applicable and can be scaled or altered to fit company needs.
- Process consistency is imperative to a program's success. Because many government programs require paperwork and electronic data transfer, industry and government programs must be amenable and must create a safe place to store PII.
- Clear communication among all departments of a company's CJIS operation must be maintained for process efficiency and to maintain trust when handling PII.

Important:

- This playbook outlines general best practices. Be sure to check with the CJIS System Agency in each state to verify its requirements and procedures.
- There are practices in this playbook that are stricter than what the current CJIS security policy requires, which maintains safety among all users in the program.
- For more information on the CJIS security policy, visit https://www.fbi.gov/services/cjis.

3 | Play 1 - Centralizing Your CJIS Management

From a high-level approach, CJIS adjudications should be managed by a single department in a company (referenced as "CJIS Operations Team" in this document).

This approach eliminates confusion, ensures consistency for streamlined processing, and ensures the successful implementation of standardized procedures.

Centralizing CJIS management also applies at state level. Company staff should ask for reciprocity in each state regarding CJIS adjudications, when permitted. This allows a single state-level entity to manage all adjudications for all jurisdictions/municipalities, with each municipality agreeing to accept state-level adjudications to allow for local CJIS access. For example, California currently has one state-level entity to finalize its state adjudications.

Checklist:

- Research whether other companies in your state submit candidates for CJIS background vetting.
- Identify key partners between your company and state adjudicators.
- Locate other teams at your company (if any exist) who are also vetting candidates for government services or customers.
- Research the number of company customers and stakeholders who must meet CJIS background check requirements.

Questions to Consider:

- Are there current relationships in place to request reciprocity for candidates applying for CJI access in the same state?
- Does your company have an existing infrastructure or a starting point for a CJIS Operations Team?

4 | Play 2 - Determining Your Company's Organizational Structure

The CJIS Operations Team should be created and located—as appropriate with the company's existing structure and culture—such that it can provide the necessary oversight, authority, and influence over company elements that operate in the CJIS environment. Various team members should consider the nature of a CJIS engagement, including:

- Corporate Security
- Chief Information Officer (CIO)
- Chief Technology Officer (CTO)
- Chief Information Security Officer (CISO)
- Legal
- Human Resources

Structuring a Single Operations Team

Ideally, a CJIS Operations Team would support the entire company. This would comprise a single team lead and additional team members who operate at current scale. Each member should be capable of performing all CJIS-related tasks with flexibility during periods of higher volume or in the event of staff absences.

A single CJIS Operations Team also helps streamline all correspondence. A single mailing address, phone number, and "Team Level" email address can then receive all communications, whether internally (from business groups and/or candidates) or externally (from state agencies/CJIS Teams).

While CJIS standards tend to stay consistent, state-specific agency requirements are often diverse. If the team has flexibility with its time, then assisting with managing FBI CJIS and state-specific requirements will consolidate efforts for their candidates. As a result, candidates will complete requirements, receive state decisions, and quickly receive CJIS data access. Current recommended capabilities include Citizenship Verification (if U.S. Citizenship is a corporate requirement) together with Corporate Policies/Guidance, and possibly having a Notary Public on staff. Certain states, such as Alabama and Minnesota, require notarized signatures on CJIS paperwork applications.

Outside of the team, a single CJIS point of contact (POC) should be designated in each supported business group in the company. This individual is referred to as the "CJIS Screening Project Manager (PM)" or "CJIS Champion." All communications to and from the CJIS Operations Team will flow through the CJIS Screening PM to verify requests and actions and to prevent confusion in communications.

The CJIS Screening PM is responsible for managing delinquencies within their own business group and communicating adjudication statuses (approvals/denials) to candidates.

Dedicated and Restricted Office Space

The CJIS Operations Team office must be in a secure area with access granted only to CJI/PII authorized personnel. Badge control to the secure access area is recommended, along with locks for any cabinets or files containing PII.

All PII forms should be organized in a way that prevents immediate viewing access. The area door must remain locked when the room is unoccupied. Locks and keys should be created separately from the master or janitorial keys.

Refer to CJIS Security Policy 5.10.1.2.2 for proper encryption techniques when digital or material CJI formats cannot be protected as recommended above.

Hours of Operation

When unvetted individuals need access to the CJIS Operations office (e.g., a janitor or a candidate applying for clearance), a member of the CJIS Operations Team must always be present with the individual. Office hours should be printed on a visible sign and/or on a website (or in the signature blocks of outgoing CJIS Operations team members' emails) to ensure available support. The team can also offer to schedule appointments on an internal website. A secure drop box can be used for candidate paperwork submitted after business hours.

Checklist:

- Identify the CJIS Operations Team, their lead, and the business element who will manage PII.
- Appropriately locate the CJIS Operations Team and communicate their availability.
- Coordinate communication and create templates for regular correspondence with candidates, their managers, and CJIS Screening PMs.

Questions to Consider:

- How will a new CJIS Operations Team fit into your existing company's structure?
- Will the team require special certifications (e.g., Notary Public, Citizenship Verification Delegate)?
- Is the required infrastructure already available to securely store PII?
- Do candidates and supporting teams understand where and how to visit and communicate with the CJIS Operations team?
- Consider the company's CJIS need and scale. Will additional business group representatives or project managers need to be hired to organize a CJIS organization across the company?

5 | Play 3 - Understanding Candidate Requirements for CJIS Compliance

Base Requirements for CJIS Compliance

The primary elements required for personnel to achieve/maintain CJIS compliance include completing a CJIS training and certification, fingerprinting, FBI CJIS Security Addendum Certification, and any state-level requirements.

CJIS Training and Certification

CJIS training is required within the first six months of CJI environment access and is required biennially. There are four levels of CJIS training. To keep candidates up-to-date and knowledgeable on the data they access, companies should require the completion of Level Four Security Awareness Training. Additionally, requiring all personnel to complete the highest training level eliminates the need to track training levels and ensures that they are trained for their role in the company.

Fingerprinting

While fingerprints are usually obtained at a local law enforcement agency via fingerprint cards, some states and agencies may allow fingerprint collection from authorized fingerprint channelers. Depending on the state agency and the fingerprinting channeler, fingerprint submissions can be sent via hard card or electronically.

Requiring all candidates to complete fingerprinting every 18 months ensures consistent quality in case of any changes, such as scarring, loss of a finger, or any other fingerprint quality changes.

FBI CJIS Security Addendum Certification

This certification is signed by the applicant who recognizes upon signing that they reviewed the CJIS security policy and understands that misusing CJIS information will result in employment termination and potential prosecution. This is a document produced and required by the FBI CJIS Division throughout the entire CJIS community.

The CJIS Operations team must obtain certification copies (available on the FBI website) for each candidate applying for CJI environment access. Original hard copies of the CJIS FBI Security Addendum Certification must be kept on file for at least one year. Some CJIS state-level background checks require additional copies, so it is also recommended to scan copies of each candidate's certification into a secure, internal site for easy access by states if required.

A new certification version is made available annually on the FBI CJIS website approximately in June. The CJIS Operations Team should download the updated copy each year to maintain an updated form for distribution.

State Requirements:

In addition to the base requirements listed on the previous page, states may also require:

- Format of fingerprint cards (hard copy or electronic)
- The number of fingerprint cards required
- Maximum “age” of fingerprint cards (based on the date completed)
- State-specific application(s)/forms
- Current copy of driver’s license or state-issued ID
- Copy of birth certificate or current passport
- Stamp(s) (e.g., ORI, POC)
- Communication through state-specific protocols

Checklist:

- Dedicate secure locations for copies of all documentation.
- Identify all requirements necessary for candidates to complete.
- Determine requirement deadlines and renewal requirements, if applicable.
- Proactively select third-party CJIS training providers and fingerprinting channelers to ensure process consistency, if authorized.
- Visit vendors to understand their processes.

Questions to Consider:

- How will candidates be notified of their requirements?
- What follow-through / insurance of requirement completion will the team implement?
- What kind of tracking process will be used to monitor requirement completion and compliance?

6 | Play 4 - Designing Tooling / Systems Technical Infrastructure

Tracking and Reporting

A single location/tool is recommended for record maintenance. This could be a spreadsheet or a relational database using employee ID numbers as differentiators.

For larger CJIS programs, a Customer Relationship Management system (CRM) and/or a workflow application is recommended. Review existing infrastructure to coordinate with:

- HR Management Systems
- Identity Management Systems
- Access Control Systems

The ability to create workflows, such as tiered approvals and auto-generated emails, will reduce the amount of manual tracking required, as these notifications can be automatically sent rather than requiring regular review and manual updates from the CJIS Operations Team. Defining role-based access and permissions will also assist in the breakdown of work so that each member part of the CJIS adjudication process can contribute to the overall process. Those with managerial permissions may also be able to track their own candidates through this process.

Items to Track

The status of the following prerequisites must be tracked for each individual candidate for initial CJIS compliance and submission:

- Citizenship verification (if required)
- Driver's license/proof of identification
- Fingerprint dates
- CJIS security training completion dates
- Signed FBI CJIS addendum
- Any role-based and/or state-specific requirements
- Ongoing CJIS qualification, as employees who were arrested, charged, or convicted of a crime can be removed from a company's CJIS program

State-specific Submissions

Candidates' statuses must be tracked for each state in which they applied for clearance. This includes tracking candidates who receive a notice of state requirements and completing them on deadline, the CJIS Operations Team who processes requirements, and the team who submits the candidate information to each state.

Once requirements are submitted to the state, the state provides the CJIS Operations Team with an "Approved," "Denied," or "Resubmittal Required" result for each candidate. Common resubmission requirements include low-quality fingerprint card submissions or incorrect/incomplete state paperwork applications.

Role-specific Access

Workflow tracking processes should establish role-specific access assigned to each employee in the program. Each level will allow employees to access what they are required to update or monitor. The CJIS Operations Team should have full access over the workflows, as they must edit permissions, initiate onboarding, and terminate candidate records. They must also view all role-based assessments for the training and troubleshooting of other users. Establishing role-based access profiles in the workflow allows for managers to monitor their employees' statuses, employees to monitor and track their own status, and to restrict access overall on a "need-to-know" basis.

Screening Managers

Managers assigned with screening potential CJIS candidates should be able to view all applicants they manage. Though the CJIS Operations Team should be the sole entity for granting entrance into the CJIS program, managers should communicate the initiation and termination of candidates from the program. Managers should not be given access to PII; they should only have access to monitor CJIS compliance statuses for those they manage.

The ability to create compliance reports for candidates is also helpful for managers. This way, they can ensure all candidates are current with their CJIS requirements, track those who are not compliant, and keep a current applicant roster for the program.

Individual Applicants

Individual applicants should have access only to what pertains to them. They should also be able to edit their own PII (upon initiation into the program and if any changes occur) and their overall CJIS compliance status. This includes their base requirements (fingerprinting and training) and their application status for each state.

Links to helpful resources should also be provided. This could include their CJIS training, fingerprinting instructions, and where to access each of their required applications.

External Customers (State Agencies)

State agencies should have access to the full roster of applicants submitted to their state. Some online applications share access to such information and can act as a records system for state agencies and the CJIS Operations Team.

This type of function provides real-time visibility into applicant status for the state and the company. The CJIS Operations Team can update the roster for each application sent to the state. The state agency can then review, update adjudication statuses, and leave notes within the roster for the CJIS Operations team to view and act upon. This function also eliminates confusion associated with communication via email or regular mail.

Reports to Create/Send Out

Generating reports allows for centralized data to be analyzed and interpreted. Workflows should be able to generate customizable reports that cater to different stakeholders. Any reports created would display original workflow data into the necessary categories.

Business Group Reports

The CJIS Operations Team should run reports for individual business groups for which they manage compliance. These reports can be used at various levels, including from high-level percentages of overall compliance to a more detailed tracking of individual applicants. Helpful data categorization abilities include the compliance status for base requirements, state submission statuses, and current employee rosters. If the CJIS Operations Team creates aging/delinquency reports, they can easily review non-compliant candidates and how long they are delinquent.

State Reports

The CJIS Operations Team should also be able to run reports by state. These reports allow the team to review and monitor that each state completes background checks and quickly communicates the results to the CJIS Operations Team. This would also enable easy access to all employees pending adjudication per state. The CJIS Operations Team could then reach out to the appropriate POC for a check-in.

Termination Reports

Individuals who do not support their CJIS program must be reported to all state agencies involved. The ability to run termination reports provides the CJIS Operations Team with a list of applicants who are no longer in the program. This report initiates the process for removing candidates from the program and notifying the states of those removed.

Fingerprint Completion

Where permissible, use nationwide fingerprinting services/channelers to collect and send out candidate fingerprints. This eliminates the need for individuals to locate local fingerprinting locations and allows for centralized billing and payments.

Fingerprint cards can be ordered from the provider as needed for submission for new background check requirements.

Depending on the state agency and the fingerprinting channeler, the fingerprint submissions can be sent via hard card or electronically. Electronic fingerprint submission is cost-effective, with fewer cards in the office, and is convenient for those involved in the transaction.

Document Management

For all required CJIS program documentation, there must be a single location for each type of document. Version control also must be maintained to ensure documents are current and consistent, and that only the CJIS Operations Team can edit the documents. Others who may require access to these documents can view and download as necessary.

The organization of all documentation is helpful for daily maintenance and if PII must be moved to a new location (i.e., physically and/or electronically). The location for each PII should be defined for the security of all applicants.

Fingerprint Cards

Fingerprint cards should be ordered from designated vendor(s) when applicants begin their CJIS adjudication process. Order enough cards to cover the minimum amount necessary for the state requirements involved in the program, and to have an inventory supply in the CJIS Operation Team's office. Should you expect additional states to onboard, maintaining this inventory will help to implement new state requirements.

Store fingerprint card copies in locked file cabinets until paired with applications for shipment.

State Submissions

To ensure consistency and accuracy, create templates for candidate correspondence related to general CJIS prerequisites (For example, citizenship verification, fingerprinting, CJIS training, and completion of the FBI Security Addendum) and state-specific applications and requirements when possible. These include notification templates for initial candidate onboarding, required resubmissions, maintaining compliance, onboarding of new states, relaying state decisions of candidate submissions (e.g., "Approved"/ "Denied"), and process instructions for appealing denials.

To reduce state rejections among candidates due to paperwork application errors, instructions for applications should be provided along with completed application examples and an FAQ with common issues.

Pre-populating an applicant's personal information in forms is also recommended. This can be completed in a single document with all the necessary paperwork included. As the number of customers served by a company increases, this function will become increasingly more important. A comprehensive form for all required applications improves accuracy and efficiency in the process.

Receipt/Transmission/Dissemination Logging

Tracking each step of CJI dissemination and storage among organizations is imperative to ensure FBI and CJIS policy compliance and for auditing purposes.

Checklist:

- Based on current size, approximated growth, and resources, determine the appropriate tools to use.
- When selecting fingerprinting and CJIS training third-party providers, locate archives for reviewing candidates' statuses of completion.
- Define and record where each type of documentation will be located.
- Review what type of reporting will be required for each stakeholder.
- Determine how the agency can physically and electronically store current and future data.
- Ensure applicant PII remains consistent in all databases for all stakeholders.

Questions to Consider:

- What sort of resources, electronic systems infrastructure, and physical document storage are already used in the agency that could be used for the CJIS Operations Team's purposes?
- Should a new state onboard with the CJIS program, what systems and organizational structures can be put in place to avoid redundancy for applicants and remain efficient for the CJIS Operations Team?
- Should the CJIS Operations Team's information be audited, and will the selected organization be sustainable for later research?
- Has the CJIS security policy been reviewed to ensure current compliance for documentation storage?

7 | Play 5 - Developing and Sustaining Ongoing Communications

Internal Communication

Recurring meetings with the CJIS Sales team and Business Groups (CJIS Screening PMs) are crucial for ongoing communication and collaboration. Monthly meetings with the CJIS Sales team provide insight and clarity into future clearance requirements. Bi-weekly correspondence with Business Groups allows for discussions on current and future CJIS applicants, upcoming clearance requirements, applicants who are non-compliant with CJIS policies, and the overall program status/performance.

A monthly internal newsletter can provide state POCs, Business Groups, and managers with up-to-date policies and process changes managed by the CJIS Operations Team. Quarterly CJIS newsletters provide updates, including ongoing and resolved internal/external issues, policy changes within CJIS Operations, real-time shared document repository access, options to move from hard card fingerprints to electronic, and an opportunity to provide feedback to improve CJIS Operations process and execution.

External Communication

Communications containing PII must be provided with additional security. Emails that contain PII must be encrypted, with the password sent in a separate email. Hardcopy paperwork should also be sent with overnight tracking information and provided to the sender and recipient.

All team members should have access to a team email address for correspondence with individuals who send CJIS inquiries. The team email address allows all team members to ask and answer CJIS-related questions and avoids situations where a team member's absence affects communication with internal and external stakeholders.

All sent applications/fingerprints/security agreements and other required documentation should be coordinated with the state and CJIS POCs. The shipment of completed applications can be determined by desired frequency, volume, tracking requirements, and specific document requirements, such as preregistrations and hard card or electronic fingerprints. Hardware sorting and storage components, such as filing cabinets and vertical hanging filing units, help organize files by storing and sorting all paperwork, fingerprint cards, and accompanying documentation from start to finish in the CJIS application process.

Checklist:

- Identify timing and schedule meetings with all internal/external stakeholders.
- Decide how information will be easily shared among POCs, whether by newsletter, flyer, or email.
- Create communications templates and establish a regular vocabulary for clear communication.

Questions to Consider:

- How will documentation (i.e., hard copy and electronic) be securely sent to state POCs for adjudication?
- Are there any POCs or business groups who require additional time due to size, Screening PM availability, or for other reasons?
- Are the CJIS Operations team's processes regularly reviewed for consistency, redundancy, and an actual need for each POC?

8 | Play 6 - Coordinating Continued CJIS Compliance and Growth

State Adjudication Protocol

Adjudications from state entities should be recorded for notifications between the employee and the manager, as well as for historical tracking. Approval notifications can be communicated to applicants, managers, and business groups via email.

State rejections should be kept confidential until the CJIS Operations Manager sends them through the chain of command and appropriate HR channels before an employee is notified of the rejection.

State Point-of-Contact (POC) Relationships

The CJIS Operations team should work with a POC in each state. Designated POCs are the appropriate first contact for all inquiries, protocol methodologies, notifications, and general communications. State POCs direct protocol for submitting required documentation.

The CJIS Operations team should provide a master reference list of all state POC information for administrative reference and to ensure continuity in communications.

Although record keeping compliance in administrative operations is outside of the scope of CJIS policies covered under the 13 policy areas for data security standards, administrative personnel must comply with administrative operations per company standards and state requirements for verifying, documenting, retaining, and executing current and legible documentation.

State FBI Criminal Justice Information Services Security Addendum

Document should be completed and submitted to the state or held on CJIS team's data repository for verification of acknowledgement by all contractor employees to abide by the content of the FBI Security Addendum.

Identification Documentation

Current state-issued driver's licenses or government issued identification cards, a U.S. Passport or U.S. Passport Card, and birth certificates are common forms of ID required with state applications.

State CJIS Online Training and Certification

CJIS online training, which is offered by a selected company, provides guidance on agency-wide security protocols and requirements. Contractor employees who complete the companion test receive a CJIS training certification confirmation which is valid for two years. Before a certificate expires, employees must recertify by completing the CJIS online training and test. Current certification verifications can be uploaded to a CJIS team repository site with certification statements for state reference.

Fingerprint Collection

Current fingerprints are required for CJIS background checks, which are based on cross-referencing applicants' fingerprints with a database. Each state determines the fingerprinting date and whether it is current or expired.

Engagement with New States

Internal Considerations

Before engaging with a new state, an internal CJIS Operations team meeting should include:

- Availability for processing submissions
- Submission cadence by individual business group or the general population
- Announcements for new state engagements via email to identify new state requirements or any specific processes to follow and schedule for submission
- Draft instructions for new state paperwork
- Review timeline requirements for submission of newly added state paperwork
- Map all submission deadlines while considering upcoming holidays, administrative staffing requirements, labor intensity for application requirements, accompanying required documentation, labor intensity for application review and submission, and any additional state requirements (for example, fingerprint registration steps and fingerprint date or expiration requirements).

External Considerations

New states contracted in CJIS environments benefit from an initial CJIS team conference call or in-person meeting to introduce and discuss state policies and procedures. The following items should be reviewed when onboarding a new state:

- Review state application paperwork, accompanying documentation, and/or supplemental state requirements.
- Discuss administrative procedures and submitting paperwork and fingerprint cards.
- Discuss submission cadence with state, including delivery methods, a secure mailing address, and the POC to receive submitted state paperwork.
- Agree on notification procedures from the state regarding approvals, denials, and any required resubmissions.
- If applicable, invite POC to access CJIS Operations team's repository for the current statuses of all applicants sent to the state.
- Share forecast numbers for initial applicant submissions and average number of submissions.
- Confirm subsequent schedule for monthly submissions, expected turnaround time for state background check completion, and discuss ongoing CJIS program.
- Designate specific state POC or specific contacts, if any, for individual communications related to submissions, adjudications, denials, and removal notifications

Resubmissions and/or Follow Up With States

As new states onboard or as applicants resubmit any documentation, templates should be documented and saved for easy access by the CJIS Operations team, including:

- Announcement of newly onboarded state(s), along with new requirements, how to properly implement them, and important deadlines
- Follow-up on requirements if not completed by the deadline
- Corrections required for any submitted state documentation

- Printing issues
- Missing documentation or fields
- Expired fingerprints or expired CJIS training certifications.

Checklist:

- Create a master reference list of state POCs.
- Schedule meetings as needed to ensure POCs and the CJIS Operations team understand expectations.
- Review documentation retention policies and procedures.
- Create templates for consistent communication.

Questions to Consider:

- How will applicants be notified of their state adjudications and denials?
- Should a new state onboard, how prepared is the CJIS Operations team to send applicants to the new state?
- Are all applicants current on their requirements, and how will the CJIS Operations team notify them if they are not?
- What sort of deadlines will be put in place for each type of requirement, and at what point will applicants be removed from the program due to noncompliance?

Appendix: Frequently Asked Questions (FAQs)

Whom is the CJIS Playbook for?

Companies with staff who create or maintain a CJIS operation where clearance is required to access a CJIS data environment to perform their job

Where can I find more information on the CJIS security policy?

The FBI includes the entire CJIS security policy on its website. You can also review your state's requirements by visiting the agency where you submit candidates for approval or rejection for CJIS data environments.

What are the base requirements for an applicant entering the program?

Per CJIS policy, these include completing fingerprinting, CJIS training within six months of entering the program, and by signing an FBI CJIS Security Addendum Certification. Other requirements may be set by each state.

How do I keep PII safe?

Review the CJIS security policy to understand what is required and keep accessibility to the CJIS Operations space to a minimum. Only those who are cleared may access PII. Review "Role-Specific Access" on page 12.

Should applicants be removed from a CJIS program for noncompliance?

Deadlines can be strict depending on the company, but it is recommended to remove applicants who were given ample time to complete their requirements and have not done so. To keep CJI secure, applicants must be compliant and aware of the sensitive data they may access. If a CJIS Training Certification expires, or if any core base requirements are incomplete, access to any CJI data must be removed until the expiration/incompletion is corrected.

Resources:

Criminal Justice Information Services (CJIS) Security Policy, (2019).
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

“Criminal Justice Information Services (CJIS).” FBI. Federal Bureau of Investigation, May 3, 2016.
https://www.fbi.gov/services/cjis

State Background Check Guide. State Background Check Info Guide. IJIS Institute. Accessed 2019.
https://ijis.site-ym.com/page/backgroundcheckinfo