

NCIC/DCIN/Nlets Systems Access Request for License Plate Reader

Questions: ARAHelp@ncsbi.gov

Technical Questions: servicedesk@ncsbi.gov

Request:

A letter of request from your agency head, on agency letter head, is required. The letter of request should include the project description, timeline, project goals, agency point of contact, vendor details and any supporting documentation if applicable. There is no specific format required. Mail request letter to:

North Carolina State Bureau of Investigation
Criminal Information and Identification Section
3320 Garner Road
PO Box 39500
Raleigh, NC 27626-0500
Attn: Compliance Unit

New:

CJIS Security Policy and Vendor Information: - Changed on March 21, 2022

Background checks on vendors who have access to criminal justice information (CJI) must be fingerprinted.

The Federal Government passed the National Crime Prevention and Privacy Act of 1998 and left it up to each State to later ratify it. One of the things the law did was establish a national fingerprint repository for things like background checks for non-criminal justice purposes. North Carolina has never ratified it (along with a handful of other States) and as a result the State does not share fingerprint data with the rest of the Country. This necessitates that all Criminal Justice Agencies in our State with access to Federal CJIS Data, fingerprint all vendor employees each and every time they enter into a contract with a new agency, even if they have done it elsewhere in the State or Nation.

Note:

At later stages in the process, our IT staff will work with agency-selected vendors to implement solutions at the agency level. The SBI does not endorse individual vendors, products or services and does not advise technology users that any one vendor is rated higher than another.

Please include your agency TAC/POC on any activities that will impact agency access to NCIC/DCIN/Nlets.

What does a law enforcement agency need to maintain on file if they use a private IT Contractor/Vendor?

Each law enforcement agency that utilizes a private contractor/vendor to provide IT assistance for computers containing **Omnixx Software/Mobile Data Software/CAD and LPR** must maintain on file:

- A signed copy of the FBI CJIS Security Addendum Certification for each contractor/vendor employee that provides IT assistance to the law enforcement agency.
- A fingerprint-based background check of each contractor/vendor employee that provides IT assistance to the law enforcement agency
- Security Awareness Training and viewed (CJIS Online) and by each contractor/vendor employee that provides IT assistance to the law enforcement agency

(Only employees that will actually be providing the IT assistance to the law enforcement agency need to complete the above documents.)

Each law enforcement agency that utilizes a private contractor/vendor to provide IT assistance with computers containing **Omnixx Software/Mobile Data Software/CAD and LPR** must have:

- Memo of Agreement/User Agreement between the law enforcement agency and vendor
- *Section 5.1.1.5 requires the Security Addendum (Appendix H, pages H-6 and 7) to be appended to the contract between the agency and the vendor.*
- Each vendor employee working on the contract with access to CJI must sign the certification page (Appendix H, page H-8)

What is the FBI CJIS Security Addendum?

A Security Addendum is a uniform addendum to an agreement between the law enforcement agency and a private IT contractor, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as may be required.

Who needs to sign the FBI CJIS Security Addendum Certification?

Each employee of the private contractor/vendor that provides IT assistance to law enforcement agencies with computers containing **Omnixx Software/Mobile Data Software/CAD and LPR** must sign the FBI CJIS Security Addendum Certification.

How is the FBI CJIS Security Addendum Certification obtained?

Local law enforcement agencies can obtain the FBI CJIS Security Addendum and Certification on the FBI website. It will be the vendor's responsibility to ensure that their employees sign these forms. The vendor should send copies of the signed Addendum Certification to the local law enforcement agency. The local law enforcement agency must keep copies of the signed FBI CJIS Security Addendum Certification on file for audit purposes.

Fingerprint Checks

A fingerprint-based background check must be conducted for each private contractor/vendor employee providing IT assistance to the law enforcement agency.

Complete the applicant fingerprint card as follows:

- Employer and Address: The name and address of the local law enforcement agency receiving the IT service
- Reason Fingerprinted: "Non-Sworn Criminal Justice Employee – Other"

The Applicant Unit will conduct a fingerprint-based background check. The Applicant Unit will send the local law enforcement agency a letter of fulfillment. The local law enforcement agency must maintain a copy of the fingerprints and a copy of the letter of fulfillment for audit purposes.

Security Awareness Training

Security Awareness Training (CJIS Online) must be taken by each contractor/vendor employee that provides IT assistance to law enforcement. This training must be taken annually.

What is a Memo of Agreement/User Agreement?

This is an agreement between the local law enforcement agency and the vendor company. The Memo of Agreement/User Agreement is prepared by the agency and the vendor. Sample agreements from the FBI can be emailed to the local law enforcement agency upon request. Please contact the Compliance Unit for an example, if needed. The Memo of Agreement/User Agreement must be kept on file by the local law enforcement agency for audit purposes.

What's Next

Once a request is received, it is reviewed internally. For a project like this, the FBI requires an external review. An MOU between the SBI, the FBI designee for North Carolina, is required. After a signed MOU is completed, agencies will then work with IT staff to implement the technology request.