

TIES VENDOR OVERVIEW

This document provides an overview of the program put into place by the Tennessee Bureau of Investigation (TBI) for approving TIES / NCIC application software. The vendor approval program applies to all vendors offering products or services to any agency within the state of Tennessee if those products or services consist of software applications that access the National Crime Information Center (NCIC) or the Tennessee Information Enforcement System (TIES).

Access to TIES and NCIC provide Tennessee agencies with vast amounts of criminal justice information which can be instantly retrieved by and/or furnished to any authorized agency. It is TBI's intent that each authorized Tennessee agency have access to all the capabilities provided through TIES and NCIC with the ultimate goal of officer and public safety. In order for this to be realized, TBI must ensure that all vendors providing TIES / NCIC software applications in Tennessee be compliant with all the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) requirements as well as TBI's requirements.

The current version of this document, as well as any of those referenced herein, is available for review and downloading from the TBI web site (www.tbi.tn.gov). Navigate to the Information Systems Division (left side), Law Enforcement Support Unit, TIES Software Vendors.

WHY DOES TBI HAVE A VENDOR APPROVAL PROGRAM?

- Meet Tennessee TIES agencies expectations for TBI guidance in selecting among vendor offerings.
- Meet FBI CJIS security requirements (Security Addendum, background checks, encryption, etc.).
- Ensure agencies have adequate helpdesk support of the vendor's application software.
- Ensure vendor software provides all transactions available (including images) for the type of access specified.
- Ensure vendor software is upgraded in a timely manner when necessary to meet changes mandated by FBI CJIS modifications to the NCIC transaction codes, revisions in CJIS policy, upgrades to the NCIC architecture, or changes made by TBI to its information systems.

VENDOR APPROVAL PROGRAM TIMELINE

The vendor approval program will be phased in by the middle of 2015.

Effective **April 30, 2014**, all vendors that do not have a signed contract with a Tennessee TIES agency for supplying software that accesses NCIC/TCIC via TBI will be required to comply with the vendor approval program. Permission will not be granted for any vendor customers to connect until the approval process has been completed.

Vendors with an active contract in place prior to **April 30, 2014**, with one or more Tennessee TIES agencies will be required to complete the vendor approval program before **April 30, 2015**. After that time, no new customers will be allowed to connect with that vendor's application software and no existing customers will be allowed to add additional devices using the vendor's software until the approval process has been completed.

TBI VENDOR USER AGREEMENT

Effective immediately, all vendors will be required to complete a formal vendor user agreement with TBI. One of the specifications in the agreement is that the vendor understands and agrees to the approval program and the criteria that will be used to determine approval by TBI.

Completion of the FBI's Security Addendum is a condition of this agreement. The addendum will be between the vendor and TBI and will substitute for the requirement that an addendum be completed between the vendor and each agency that uses its software applications.

This agreement will apply to all vendors presently doing business within the state as well as those that may wish to do so in the future.

TBI VENDOR EMPLOYEE REQUIREMENTS

The vendor employee requirements apply to all vendor employees having direct responsibility to configure and maintain computer systems, software, and networks with direct access to Criminal Justice Information (CJI).

Fingerprint-based background checks will be required on all applicable vendor employees. These fingerprint cards must be submitted to the TBI, with the "reason fingerprinted" stating Contract Employee and the name of the company. Two sets of prints for each applicable employee must be submitted at a cost of \$60.00 per employee. Checks should be made payable to the Tennessee Bureau of Investigation (TBI). The TBI will issue fingerprint cards for this purpose.

- A vendor employee found to have a felony conviction will be disqualified.
- A vendor employee will also be disqualified if an arrest warrant is confirmed to be outstanding.
- A vendor employee with a misdemeanor offense(s) may be granted access if the CJIS Systems Officer (CSO) determines the misdemeanor offense(s) do not warrant disqualification.
- Background re-investigations may be conducted by the TBI on applicable personnel every five years.

Applicable employees of the vendor must complete a TIES Vendor Employee Eligibility Form and submit a copy of their driver license.

Fingerprint submissions for all applicable employees hired in the future must be submitted to TBI with noted fees and the TIES Vendor Employee Eligibility Form for processing within 30 days of assignment.

All applicable vendor employees must read the CJIS Security Addendum (appended to the user agreement) and any other pertinent documentation provided by TBI. Each employee must sign the CJIS Security Addendum Certification Form (appended to the user agreement), acknowledging that they recognize that CJIS systems data is sensitive information, and security shall be afforded to prevent any unauthorized access, use, or dissemination of the information. Improper access, use, or dissemination of CJIS systems data is serious and may result in the termination of services and/or state and federal criminal penalties.

Security awareness training is required within six months of initial assignment, and biennially thereafter. This training should be completed on-line via CJIS Online (www.cjisonline.com).

Instructions for completing this training process will be provided to the individual listed as the vendor's point of contact for TBI.

TIES SOFTWARE APPROVAL LEVELS

For TIES software, three levels of approval are supported: Mobile / CAD, Query-only, and Full Access.

TBI will provide a list of transaction codes for each level. To meet approval, the vendor's application will be required to properly process the transactions specified by TBI.

The vendor may extend this minimum set to include other transactions to meet customer needs or market expectations. Any such extensions must be provided to TBI and will be subject to the approval process.

All vendor TIES software is now required to provide the capability to view images and full access software must provide the capability to also enter images.

APPROVAL COSTS

TBI will not impose on any vendor a fee for approval or require any fee to maintain an approved status. However, the vendor is responsible for all charges related to the fingerprint background process.

REQUIREMENTS FOR TIES SOFTWARE APPROVAL

1. Submit a Vendor Profile Form and letter of request to access the TIES network. This form must also include all pertinent information regarding the company and its products, a list of all states that the company currently has contracts with, and a list of all Tennessee agencies that are current customers.
2. Must pass transaction tests (Mobile / CAD, Query-only, and/or Full Access).
3. Transaction response times must meet NCIC specifications.
4. Helpdesk staff available: Query only must be available during normal business hours and Full access must be available 24 hours a day, 7 days a week.
5. Must agree to test with TBI (in the test environment) all required modifications to specific transactions and once approved, distribute to all devices running the vendor's software, within the specified time frame established by TBI based on statutes or FBI regulations. TBI will contact the vendor regarding updates using the information provided by the vendor on the Vendor Profile form.
6. Must have a completed TBI Vendor User Agreement and CJIS Security Addendum on file with TBI.
7. A signed Security Addendum Certification Form for each employee must be on file with TBI.
8. Employees must have fingerprint background checks successfully completed and on file with

TBI with no prohibitors found.

9. Employees must have successfully completed security awareness training and testing via CJIS Online (www.cjisonline.com). Additionally, this training and testing must be completed every two years thereafter.
10. For mobile and query-only access, the capability to view images must be available. For full access, the capability to enter and view images must be available.
11. Data must be encrypted while in transit and at rest. Encryption shall be a minimum of 128 bit and certified to meet FIPS 140-2 standards. A list of the certified encryption implementations along with the NIST certificate numbers must be provided to TBI.
12. Software used to access CJI shall follow the secure password attributes below to authenticate an individual's unique ID. Passwords shall:
 - Be a minimum length of eight (8) characters on all systems
 - Not be a dictionary word or proper name
 - Not be the same as the User ID
 - Expire within a maximum of 90 calendar days
 - Not be identical to the previous ten (10) passwords
 - Not be transmitted in the clear outside the secure location
 - Not be displayed when entered
13. Advanced Authentication must be available as mandated by the CJIS Security Policy, which currently states, *“Advanced Authentication will be required for all law enforcement personnel accessing NCIC criminal justice information outside of a secure location.”*
14. Provide Administrator, Domain Manager and user settings to allow for administrators to audit and administer users.
15. Provide detailed logging, to allow user transaction auditing.
16. Ensure that automatic software updates are provided to users.
17. Provide reliable, real-time access to NCIC, Nlets & the state CJIS systems.

APPROVAL PROCESS

This section provides a brief overview of the actual approval process that takes place between TBI and a vendor. This process is subject to change as experience is gained by TBI and feedback is received from vendors undergoing the approval process.

1. Vendor completes and sends to TBI a Vendor User Agreement. As part of this agreement, the vendor must complete the CJIS Security Addendum and have completed fingerprint-based background checks on any of its personnel that will have contact with TIES / NCIC data.
2. Vendor requests approval by completing and sending to TBI the Vendor Profile form.
3. For TIES software vendors, TBI provides a list of TIES transaction codes.

4. If Mobile / CAD or Query only access, vendor must schedule a two week time frame with TBI personnel to query required transactions through the TIES test switch. TBI staff will review and make recommendations.
5. If Full access, vendor must schedule an appointment to come on-site at TBI Headquarters and complete the testing process. This process takes an average of three days. In the interest of saving time, it is highly recommended that vendor personnel on-site have the knowledge and capability to make software changes during the testing process.
6. TBI verifies responses and issues Pass/Fail.
7. If pass, TBI issues a letter of approval to the vendor (for the specific product tested).
8. If fail, TBI provides vendor a list of incorrect responses with description of errors. The vendor corrects problems and TBI personnel review. Once all transactions have been corrected, TBI issues a letter of approval to the vendor (for the specific product tested).
9. TBI adds vendor's product to approved vendor list and posts on TIESnet (TIES agency Intranet site) and the TBI Website.

VENDOR OBLIGATIONS

Upon successful completion of the vendor approval program, TBI will issue a Letter of Approval to the vendor permitting it to designate its application as "Approved by TBI". Until this letter is issued, the vendor will refrain from marketing its product as reviewed or approved by TBI.

Approval status will be withdrawn if vendors do not comply with the requirements to maintain their software to meet new or changed transaction codes, message formats, or otherwise fail to comply with the requirements for approval. Once approval has been withdrawn, the vendor will not be permitted to add new customers until approval is again obtained. TBI will notify all known Tennessee customers of the vendor's loss of approval and will not approve any new or additional connections using the vendor's software for those agencies until approval has been regained.

AGENCY AWARENESS

TBI will make a best effort to maintain a list of all known vendors of TIES / NCIC software and the compliance status of those products on the TIESnet and TBI Website. Agencies should consult that list when selecting a vendor solution for their TIES / NCIC connectivity.

All agencies are encouraged to specify TBI approval as a requirement in their RFP or contract negotiations with TIES / NCIC software vendors. In addition, agencies should consider including a clause in the contract that releases the agency from any further financial obligation to the vendor if the vendor should lose their approval through TBI.

In the event the vendor loses approval, TBI will attempt to contact every known customer to advise them of the change in status. Those customers that are already using the vendor's product will not be disconnected or forced by TBI to switch to an approved vendor. However, the agency should consider the consequences of doing business with a vendor that will not be permitted to add any new customers within Tennessee.

TBI CONTACT INFORMATION

Questions concerning the vendor approval program may be directed to Katie Chestnut at (615) 744-4072 or Katie.Chestnut@tn.gov.