Florida State University

Center for Transportation and Public Safety

www.elvisflorida.org | *www.tracsflorida.org*

FDLE Application/Service/System Audit Checklist

Traffic and Criminal Software (TraCS)

What is TraCS?

The Traffic and Criminal Software (TraCS) is a client-server based application that uses web services to communicate from the client to a web server, and from the web server to the database. The infrastructure can vary per agency.

Hosted web server and database server is either housed at the Panama City Police Department or is housed at another law enforcement agency (in-house or at your local Sheriff's department). TraCS provides electronic versions of reports typically found in a records management system, such as crash reports, uniform traffic citations, incident reports, arrest reports, and more. Not all forms are available to all agencies.

Does it process or store CJI?

TraCS does not processes CJI through messages sent and received by the FCIC message switch. TraCS has no direct access to CJI though the FCIC message switch. Not all LEAs use TraCS in a manner that stores CJI. Below is chart that describes which forms store CJI.

Form Name	CJI Stored Yes/No
DHSMV Crash	No
Tow	No
DHSMV Uniform Traffic Citation	No
FWC Boating Citation	No
DHSMV Driving Under the Influence Citation	No
Warning Citation	No
Trespass Warning	No
Parking Citation	No
Radar/Laser Log	No
DHSMV Urine and Breath Refusal	No
DHSMV Blood Refusal	No
Implied Consent	No

TraCS Traffic and Criminal Software

ELVIS Electronic License and Vehicle Information System

Driving Under the Influence Packet	No
Contraband and Forfeiture Act	No
Daily Observation Report	No
Property Receipt	No
Offense-Incident Report	Yes
Arrest-Probable Cause Affidavit	Yes
Field Interview	Yes

If it contains CJI, is it included on the agency's CSIRT plan for notifying the FDLE CJIS ISO?
For some agencies, the TraCS hardware, including the servers and network are housed at the Panama City Police Department, and is a part of Panama City Police Department's CSIRT plan. Security logs are reviewed weekly. However, TraCS should also be a part of the CSIRT for each agency that uses the system.

Is it connected to the FCIC message switch?
No, There are no TraCS computers used to communicate with the FCIC message switch through CJNet.

Can it submit queries to the message switch?
No TraCS computers are used to communicate with the FCIC message switch through CJNet.

Are access accounts set for least privileged?
Yes. By default, new user accounts are only granted enough privileges to use the system for routine tasks, such as creating new reports, searching, and printing. User accounts can only modify reports they themselves have created and have no permission to modify reports created by other accounts. Access to modify reports created by others must be granted by an agency administrator. Administrator accounts have access to create new users for their agency as well as see all user activity for their agency. Administrator access can only be given by a user that has administrator or above access.

What's the process for requesting/obtaining an account?
TraCS will create an account for the designated agency administrator so that they can create accounts for the rest of their department.

Does it comply with CSP password requirements?
Yes. Passwords must be at least 8 characters long, not the same as their user name, not a dictionary word, and not the same as any of their last 10 passwords. Passwords expire every 90 days. The user is warned 14 days prior to password expiration. Once a password has expired, the user cannot access the system until they have changed their password.

Do users share "accounts"?
No. User ID's are unique should not be shared.

What's the process for resetting passwords?
Users may reset their own passwords through the system by clicking the "Forgot Password" link on the TraCS application's sign in splash screen. They are prompted to enter their User ID and their e-mail address, and they are e-mailed a unique, randomly generated token that they must use to create a new password.

Are system user accounts validated on an annual basis?
This is up to the individual agency policy. It is recommended to review user accounts more often than the annual basis required by FDLE.

- **Is the validation process documented?**
  This is again up to the individual agency policy. Documentation of this process can be as simple as a date and name of the person conducting the review of the user accounts.

Does it deny access for a given number of unsuccessful log-on attempts?
Yes. After 5 failed sign in attempts, TraCS locks the user account for 10 minutes.

Does it have a built in session lock?
No, TraCS relies on the session lock of the operating system to comply with CJIS policy.

Does it have a system use "warning" notification banner?
No, TraCS relies on the warning notification of the operating system to comply with CJIS policy.

Is it accessed from locations other than the building where the server is located?
Yes. For agencies hosted by TraCS, the hardware is located at the Panama City Police Department. For agencies that host themselves or are hosted at another LEA, TraCS relies on the agency to comply with the CJIS policy. Many agencies across the state of Florida access it from desktops and laptops. There is not currently a version of the TraCS software available that operates on mobile devices.

Does the system/application encrypt the access session?
Yes. All traffic to TraCS is encrypted end-to-end via OpenSSL using FIPS 140-2 certified AES using 256 bit encryption.

- **Are the network lines encrypted?**
  For agencies hosted by TraCS, the network lines are encrypted at the Panama City Police Department. For agencies that host themselves or are hosted at another LEA, TraCS relies on the agency to comply with the CJIS policy.

Can it be accessed remotely?
Yes.

What is the process for remote access, e.g., IPSec VPN?
The TraCS application transmit data using web services, which is accessed via SSL encrypted connection through any modern web browser (IE 9+, Chrome, Safari, Firefox, etc.).

Can privileged functions be performed via remote access?
Yes. All of TraCS's functions can be performed remotely.

Does it use an advanced authentication process?
No. TraCS has no direct access to CJI though the FCIC message switch. TraCS users have no ability to conduct transactional activities on state or national repositories, applications, or services (i.e. indirect access) using the TraCS application. TraCS requires all authentication attempts to use both username/password combinations. It is the agency responsibility to maintain advanced authentication

(AA) on their mobile device. All mobile devices must have AA to sign in to the device, regardless of what applications they use. TraCS is not then required to have any additional AA beyond that.

- **AA Process/Method:**
  N/A.

Does it accept federated identity protocols?
No. TraCS maintains all of its own user accounts.

Is it located in a CSP defined physically secure location?
For agencies we host, yes, all of the TraCS hardware is located in the physically secure server room at the Panama City Police Department. For agencies that host themselves or are hosted at another LEA, TraCS relies on the agency to comply with the CJIS policy.

Does it include a "native" encryption feature(s)?
Yes. TraCS supports both native and third party encryption. In addition to database encryption, the messages stored in the database are encrypted at the application level before being sent to the database.

Is the encryption mechanism FIPS 140-2 certified?
Yes. Traffic between clients and the server are encrypted using OpenSSL operating in FIPS compliant mode using AES 256 or better encryption. The application itself uses Windows Cryptographic modules to encrypt the messages before they are sent to the database for persistent storage.

Do you have a copy of the FIPS certificate?
Yes. Both the OpenSSL and Windows Server FIPS certificates are available on the TraCS website for download along with this document.

Is audit logging enabled?
Yes. Auditing cannot be disabled in TraCS.

Are all applicable events logged?

Yes. Creation and modification of group accounts (agencies), creation and modification of user accounts (such as account activation and change of password), and user sign-in attempts are just a few examples of events captured by logging in TraCS.

Are all required fields captured in the logging process?
Yes. Events are tracked by date and time, user account effected, user account attempting to make the change, a description of the event, and whether or not the attempt was successful.

Does it notify you in the event of logging failure?
Yes. However, actions performed and their respective audit logging either succeed or fail together as a single transaction. An action cannot be performed at all if the act of logging it fails. If the system has been disabled to the point that logging cannot be performed, the system administrators are notified automatically by monitoring software.

Do you maintain these audit logs for at least one year?
Yes. Audit logs currently exist for at least three years.

How often are the audit logs reviewed?
This is by individual agency policy. We recommend reviewing the audit logs at least monthly.

Is it included in an established patch management process?
For agencies hosted by TraCS, the hardware is housed at the Panama City Police Department and is governed by their agency's policies for patch management. For agencies that host themselves or are hosted at another LEA, TraCS relies on the agency to comply with the CJIS policy.

Are all patches up to date?
Yes. Patches are scheduled to automatically install during low-usage periods.

Is it protected from malicious code (e.g., viruses, worms, Trojan horses)?

For agencies hosted by TraCS, the hardware is housed at the Panama City Police Department and all servers are protected by Windows Defender. For agencies that host themselves or are hosted at another LEA, TraCS relies on the agency to comply with the CJIS policy.

Is it virtualized?

For agencies hosted by TraCS, the hardware is housed at the Panama City Police Department. The web servers are virtualized and the database servers are not. For agencies that host themselves or are hosted at another LEA, it varies.

Is it at another entity's/agency's data center?

For agencies hosted by TraCS, yes, the hardware is housed at the Panama City Police Department. Some agencies host themselves or are hosted at another LEA, it varies.

Is it in the cloud?

For agencies hosted by TraCS, Yes, the hardware is housed at the Panama City Police Department and is a private cloud. Some agencies host themselves or are hosted at another LEA. In those cases, the agency would need to clarify.

- **If so, where are the data center(s) located?**

  For agencies hosted by TraCS, the Data Center is located at 1209 E 15th St, Panama City, Florida (Panama City Police Department). Not applicable for agencies that host data within a LEA.

Does it require an MCA?

Sometimes. Department heads of agencies that are hosted by TraCS that use forms in TraCS that store CJI must sign a Memorandum of Understanding (MOU) with the department head of Panama City Police Department (PCPD). Once the MOU is signed by both department heads, forms that store CJI will be made available to the agency per their request. There is also a Management Control Agreement (MCA) which is maintained between the Panama City Police Department and the Florida State University.

Does it require the security addendum process?

For agencies hosted by TraCS, yes. The security addendum is maintained by the Panama City Police Department. For agencies that host themselves or are hosted at another LEA, TraCS relies on the agency to comply with the CJIS policy.

Does it allow multiple concurrent sessions?

Yes. TraCS allows the same user to log in from multiple different devices simultaneously (such as the MDT in their car or a workstation in the agency). However, while users can log in and search for forms and print forms, they cannot 'edit' or 'create' multiple forms from multiple devices.

Is it using an XP OS?

No. TraCS is not supported on XP.

Is access allowed from a personally owned device?

No. The statewide license for TraCS is only allowed to be used by public safety officials and on department issued devices.