

## **Criminal Justice Information Technology Security Audit**

### **Answers to some of the questions**

Keep in mind that most of the questions apply to your local network setup. While LawTrak relies ultimately on your network security for the data to be secure, we do have some things in place to add another layer of security and keep some audit logs specific to the program. Most of the audit logs referred to in this audit also include server/system logs as well, which we are not responsible for.

### **Page 3:**

You will need to download the following from the LawTrak Web Site:

- Management Control Agreement
- Security Addendums
- Encryption Certificates for Bomgar

These can be found by going to <http://www.lawtrak.com> – Contact Us – Click on the link for Security Addenda, Bomgar Cert, and Management Control Agreements, and find your agency's agreement.

### **Back-up Recovery Site (disaster recovery site / where system back-ups are stored):**

This is only filled in with our information if your agency sends backups to our office through the Additional Apps.

Contact Name: Brian Lovensheimer

Title: Systems Engineer

Street Address: 220 Aberdeen Drive

City: Florence

State: SC

Zip: 29501

Phone: (843) 393-7800

Email: [support@lawtrak.com](mailto:support@lawtrak.com)

## NETWORK INFRASTRUCTURE

1. What software application(s) is used to access FBI CJIS System and/or data?

This could possibly apply to LawTrak ONLY IF you use Datamaxx Edge and run the queries through LawTrak first, and the return data comes back to LawTrak. If you are using queries to go to any other NCIC program (E-Agent, Gold Shield, etc.), we do not have the return data processed through LawTrak.

2. Does the agency store FBI CJI in a RMS/CMS/JMS or CAD system?

If you are using Datamaxx Edge with a query from LawTrak, then Yes. If you copy and paste information from NCIC returns into LawTrak, then Yes. If you call your dispatcher to run something through NCIC and then type it into LawTrak, then Yes. So most likely, the answer is Yes.

3. Which agency is responsible for the creation and deletion of system user accounts to gain access to FBI CJIS data?

The Local Agency is responsible for adding users. However, the choices given raise a question... What in the world does CSA stand for? I have found several options to choose from, but few seem to apply. Community Supported Agriculture, Comprehensive Safety Analysis, Canadian Soccer Association. The only one that seems to apply would be Customer Service Agent. I suppose that would be us, but we don't do it.

Update to this: We finally got to the Terms and Definitions section, and apparently CSA means CJIS Systems Agency. That would refer to the State/SLED.

4. Does the agency prompt a system use notification prior to providing access to systems that access, process, or store CJI?

Yes. That's the silly wording on the bottom of the LawTrak logon screen, as well as the cute little bouncing ball screen that pops up right after a successful log-in.

5. Does the agency system employ a session lock timeout after a maximum of 30 minutes of inactivity?

LawTrak does not, but your computer may go back to a screen saver with password to get back onto the system. Do NOT let the computer sleep.

6. Which agency is responsible for authenticating users to gain access to FBI CJIS data?

Both. You are responsible for making sure passwords are kept up to date for the computers/network. We make the user reset passwords every 90 days.

6b. Please provide agency's password construction requirements: (this is only for LawTrak)

How many characters? 8-15

Attributes/special characters? At least 1 letter, 1 number, 1 special character, does not include user name

Expiration? 90 days

History? Cannot use the same password until 10 other passwords have been used

6b1. How many unsuccessful login attempts are provided?

We don't limit it or lock the accounts, but we do track the unsuccessful logins.

6c. Does the agency allow remote access to FBI CJIS systems and/or data?

If you're working on a Remote Desktop, then yes. The authentication is up to you.

7. Do all applications used to access, transmit, and/or store CJI log the following:

successful and unsuccessful log on attempts – Yes

successful and unsuccessful password changes – Only successful

successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource – Only successful

successful and unsuccessful actions by privileged accounts – Only successful

successful and unsuccessful attempts for users to access, modify, or destroy audit log files – Only successful, but we do keep a history of the logs.

8. Does each audited event include:

date and time – Yes

component of information system where event occurred – Yes

type of event – Yes

user/subject identity – Yes

outcome of the event – Yes

8a. Does the agency review audit logs?

We keep them, but it's up to you to review them if you want. We don't make you do it.

8b. Does the agency retain audit logs?

Yes

8c. In the event of an audit processing failure, does the information system provide alerts to appropriate agency officials?

For LawTrak, that would be impossible. If there is an audit processing failure, 99% of the time it's due to a user dropping off the network and losing connection to the files. If the user can't connect to the files, we can't process failures.

10. Does the agency utilize CJJ related systems or applications hosted in the Cloud?

As far as I know, right now, this would only apply if you're using Datamaxx Edge.