How To Pass Your CJIS Audit

An Argent Compliance White Paper

ARGENT

Introduction

All networks have vulnerabilities. The job of IT Security groups is to minimize those vulnerabilities. In the United States, there are a plethora of compliance agencies whose sole purpose is to provide instructions that assist private and public organizations in strengthening their IT security infrastructure.

For instance, HIPAA provides regulations for healthcare, and PCI supports Internet based financial transactions.

For local, state, and federal law enforcement, the main regulatory group is the **Criminal Justice Information Services (CJIS).** For all local, state, and federal agencies, there are two key components of **CJIS: intelligence and security.**

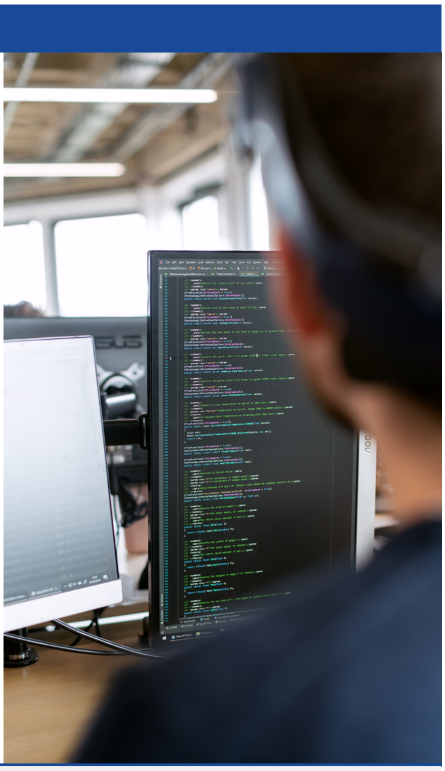
Intelligence gathering involves anything pertaining to information on crimes or suspects, such as criminal background checks or detailed records of past crimes. Security, on the other hand, is the means to ensure the privileged intelligence does not fall into the wrong hands. Intelligence must be kept secure or else it loses its value.

In today's world of social media, cloud computing, and smartphones, sharing information has become widespread and far, far too easy.

Thus the critical needs for CJIS. The huge benefits inherent in law enforcement agencies having direct access to intelligence across multiple agencies has helped bring criminals to justice swiftly. **But with this increased efficiency of sharing critical, sensitive data between local, state, and national agencies,** it has become more important than ever to safeguard sensitive data.

Data Beneficial To Law Enforcement Is Also Beneficial To Criminals

The importance of securing law enforcement data is undeniable, especially concerning interjurisdictional collaborations. CJIS Security Policy was created specifically to address this.



Implemented in 1998, CJIS policy is continuing to evolve, growing with the ever increasing digital threats we face. Although CJIS is constantly growing, the basic principle of the policy has remained the same: **To offer defined security criteria that law enforcement and criminal justice agencies must adhere to.**

In other words, all agencies with access to local, state, and federal criminal databases are subject to periodic audits to ensure compliance with CJIS policies.

What to Expect In a CJIS Audit

CJIS policy is comprehensive. And a CJIS audit is equally comprehensive; it's tough; it's serious, adult stuff; it's not a joke, and it cannot be taken lightly. But a CJIS audit can be passed with a little planning and having the right tools in place.

Listing all the CJIS requirements exceeds the scope of this White Paper. To review the latest full version of CJIS policy, go to: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

The purpose of this white paper is to address one of the central and most crucial aspects of all CJIS audits: security log monitoring. **CJIS requires all agencies and organizations to archive all the following information for a minimum of 365 days:**

Successful and unsuccessful log-on attempts

Successful and unsuccessful attempts to use, access, create, write, delete, or change permissions on a user account, file, directory or other system resource

Successful and unsuccessful attempts to change account passwords

Successful and unsuccessful actions by privileged accounts

Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file

Protect all audit logs and auditing tools from modification, deletion, and unauthorized access

Collecting and archiving this data is merely the first step to achieving CJIS compliance, as a recent Florida local agency painfully found out.

The agency, which will remain undisclosed for security reasons, was found to be out of CJIS compliance for numerous infractions. **Chief among these infractions was log monitoring and archiving.**

The sad tragedy was that the agency had completed the first step of collecting and archiving IT security events but had no way of proving this to the outside CJIS auditors. Many law enforcement agencies are not even accomplishing the first step.

So why did this agency get an "F" on its CJIS report card? When asked to give reports proving the collection of the data, the agency responded with blank stares. When asked if the agency reviewed security information gathered on a weekly basis, the CJIS auditor was met with blank stares. The agency had forgotten one simple thing: **unless you can give proof of something, it does not exist.**

No Proof = Audit Fail

Argent Reports gives you this proof in under 30 minutes. Argent comes with over 20 standard reports and Argent Reports allows agencies to instantly create customizable CJIS reports.

In a few clicks, a report can be generated showing proof that required events are being collected. Along with the creation of the reports, Argent Reports has a powerful scheduler giving IT personnel the ability to generate and email weekly or daily reports directly to a Security Officer.

As CJIS grows and expands, so Argent Reports grows alongside it.

Argent for Compliance handles **all the collection and storage of all security logs and Syslogs for CJIS.** Not merely an event collection tool, Argent for Compliance can also alert on events via seven notification methods such as email or SMS. This alerting capability allows agencies to be able to **monitor logs proactively, detecting when someone attempts to modify log auditing or commit brute force attacks** onto a CJIS system.

The alerting capability of Argent for Compliance allows agencies to report findings to appropriate officials, and ensure they are taking all necessary actions.

Combined with Argent Reports sending daily or weekly event summaries, **Argent for Compliance allows agencies to readily investigate suspicious activity or suspected violations.** Argent for Compliance not only reads and stores an agency's critical security logs but it also audits itself, logging any changes to its registry and configuration.

In short, Argent Reports and Argent for Compliance are critical for complying with CJIS Security Policy. And with Argent Reports, agencies can now easily prove to the outside CJIS auditors that all requirements have been met. In fact, as the earlier-mentioned agency found out the hard way, the inability to produce such reports to CJIS auditors casts suspicion on local Security Officers' policies and will guarantee failure by CJIS auditors and possible sanctions.

Contact your local Argent Account Manager today to find out more about implementing Argent for Compliance with Argent Reports so your agency will not become the next white paper anecdote!

Argent Software created this document for informational purposes only. Argent Software makes no warranties, express or implied, in this document. The information in this document is subject to change without notice. Argent Software shall not be liable for any technical or editorial errors, or omissions contained in this document, nor for incidental, indirect or consequential damages resulting from the furnishing, performance, or use of the material contained in this document, or the document itself. All views expressed are the opinions of Argent Software. All trademarks and registered trademarks are the property of their respective owners.