SECURELINK

CJIS compliance guide for state and local governments

State and local government agencies of all sizes rely on data from Criminal Justice Information Services[1] (CJIS) administered by the Federal Bureau of Investigation to do their jobs. Established by the FBI in 1992, the goal of CJIS is to empower state and local agencies to succeed in their missions, whether it's solving crime or protecting public safety. But information is power, and with great power comes great responsibility.

This is where CJIS compliance comes in. To mitigate the loss of sensitive federal data that can compromise public health and safety, CJIS has established regulations for government entities, as well as any contractors or third-party vendors that access criminal justice information.

For agencies and contractors that are not complying with CJIS policies, the stakes are high - violations can result in criminal penalties, loss of access to criminal justice information, and an erosion of public trust in government agencies at all levels. In the wrong hands, compromised data can impede criminal investigations, compromise federal departments including Treasury and State, and even threaten national security.

State and local governments are becoming frequent targets for several reasons

1. **Typically less secure (and less funded) than their federal counterparts, state and local agencies are seen by cybercriminals as an easy target. A report[2] that surveyed local government officials in the United States found that nearly half of the respondents indicated that their cyberinfrastructure is attacked daily, 18 percent reporting attacks every hour.**

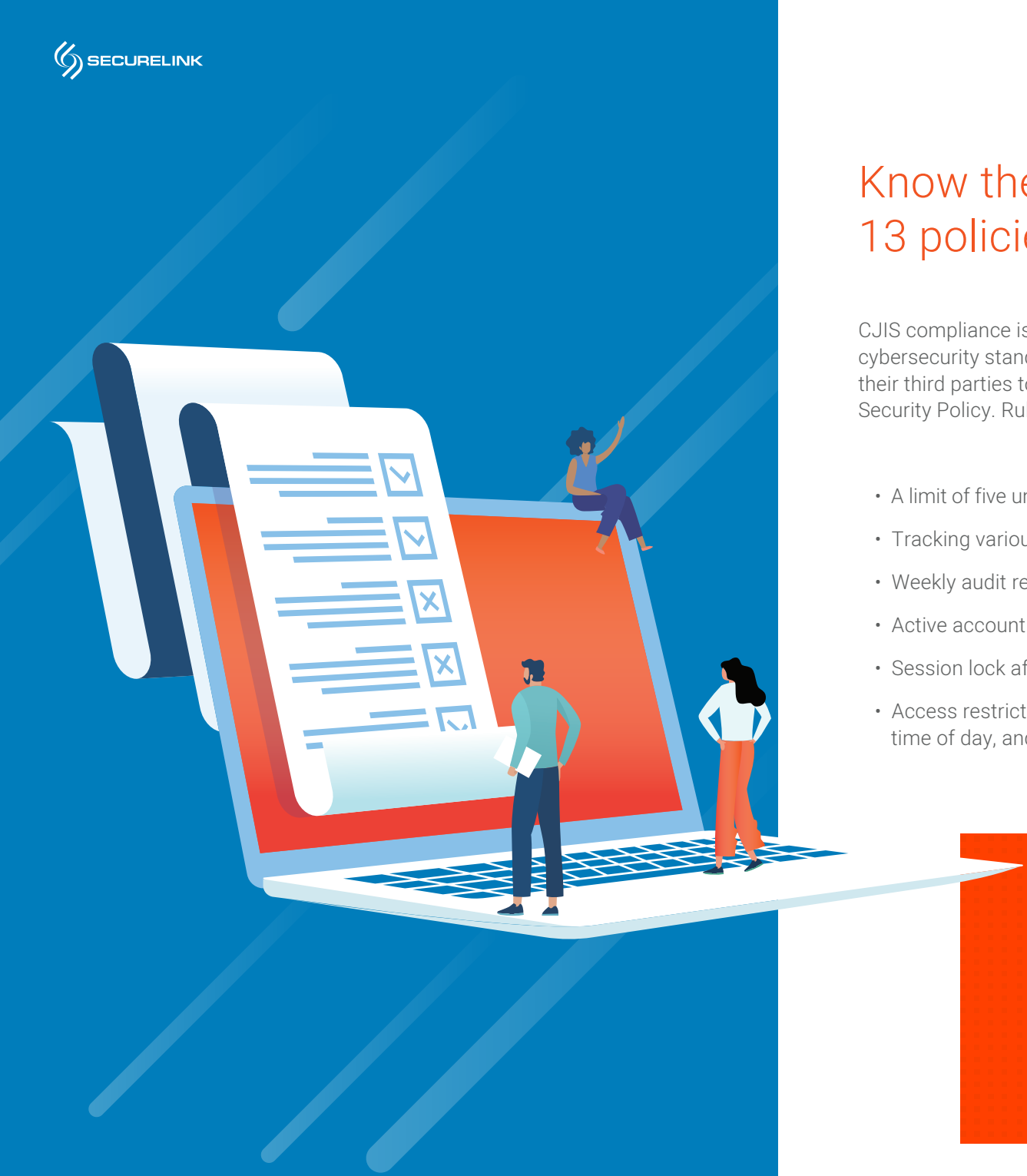
2. **Even small, local agencies can provide malicious actors with a portal into highly sensitive data within CJIS databases.**

3. **Law enforcement and public safety agencies, as well as their third-party vendors, are increasingly using mobile phones, many containing unauthorized apps, to transmit and store CJIS data.**

4. **The COVID-19 pandemic has resulted in 46 percent of state and local government employees now working at home, challenging government IT personnel to secure endpoints for remote workers.**

CJIS compliance has become more precarious as cyberattacks increase in size, number, and the amount of damage they can do. At a cool 253 pages, the FBI's CJIS document can be a daunting read, and the 13 policies surrounding wireless networking, data encryption, and remote access can feel overwhelming. Before you pull an all-nighter memorizing the CJIS Security Policy[3], read the following guide for key principles of CJIS compliance for state and local government agencies and their contractors.

[1]Criminal Justice Information Services
[2]Cybersecurity: Protecting local government digital resources
[3]CJIS Security Policy Resource Center



Know the basic rules of CJIS' 13 policies

CJIS compliance is one of the most stringent and comprehensive cybersecurity standards. That's why it's critical for governments and their third parties to know the basic rules of the 13 areas of the CJIS Security Policy. Rules of the policy pertain to:

- A limit of five unsuccessful login attempts by a user accessing CJIS
- Tracking various login activities, including password changes
- Weekly audit reviews
- Active account management moderation
- Session lock after 30 minutes of inactivity
- Access restriction based on physical location, job assignment, time of day, and network address

THE SECURELINK SOLUTION

Many SecureLink customers are government agencies or technology vendors that provide technical services for government operations. Because of this, SecureLink created a summarized synopsis of the entire CJIS Security Policy document[4] to help enterprises and vendors become familiar with the 13 policies and ensure compliance.

[4]CJIS compliance guide: 13 areas to know

Don't trust a contractor's claim that they are "CJIS-certified" or otherwise pre-approved for use. CJIS does not grant certifications.

Prepare an incident response plan

State and local government agencies must have an incident response plan (IRP) in the event of a malicious attack. The IRP must detail the agency's plans for identifying, containing, analyzing, and recovering from a data breach or attack in a timely manner.

Any incidents must be tracked, documented, and reported to the Justice Department—and this includes agency contractors and vendors. Recent data shows that approximately 60 percent of data breaches are linked to contractors and third-party vendors,[5] yet a recent Ponemon survey[6] reports that only 36 percent of respondents were confident that their contractors would notify them if they experienced a breach.

THE SECURELINK SOLUTION

If trouble does arise, government systems must trace the source of the attack and easily identify the point of entry. The SecureLink platform provides full visibility into each employee and contractor's network activity, as well as provides an audit trail of all activity while users were within the system. It also gathers granular documentation, including activity logs, video recordings, and keystroke tracking, before it's demanded

Always be prepared: Auditing and accountability

State and local government agencies should closely monitor all privileged activity to flag irregularities in requests and access. A remote-access platform that provides automated auditing, down to the granular level, will record each instance of a privileged credential in use, including:

- The name of the user
- The start and end time of the session
- Actions taken under the power of that credential

The ability to produce a comprehensive audit trail of user activity is not only mandatory for meeting CJIS compliance; it's essential to network security.[7] Further, an audit trail will assist agency employees with CJIS' formal security audits,[8] which all CJIS compliant organizations are subject to once every three years.

THE SECURELINK SOLUTION

The right remote access platform will have the features needed to deliver this level of user tracking. SecureLink provides network managers with real-time monitoring and records all activity at the individual user level to maintain clear accountability.

[5]CISOs: Make 2020 the year you focus on third-party cyber risk | [6]A crisis in third-party remote access security
[7]Why you need effective audit trails: Best practices and benefits
[8]Secure and Uncompromised Criminal Justice Information with Help from the CJIS Audit Unit

Enforce strict access control

Securing and managing users' access to information and systems within the network is paramount to meeting CJIS compliance and protecting your agency from a costly breach. The key components of access control under CJIS involve password management, configuration management, and system/information integrity protection.

IDENTIFICATION AND AUTHENTICATION

All government users, including contractors, must comply with CJIS authentication standards to access sensitive data. This requires the use of multi-factor authentication (MFA),[9] which uses two or more factors to authenticate users and eliminate shared login risks.

THE SECURELINK SOLUTION

Per CJIS requirements, a maximum of five unsuccessful login attempts is allowed per user, after which their credentials will need to be reset. SecureLink provides a safe way for third-party users to reset their own passwords. Further, agency administrators can easily manage the onboarding and offboarding of former government employees and contractors through the SecureLink platform.

REINFORCE CONFIGURATION MANAGEMENT

Only authorized users can make configuration changes to systems with sensitive criminal justice information. This includes software updates and the addition or removal of hardware.

Ensuring proper configuration management is just one of many important reasons to adopt a principle of least privilege at your agency. This security practice ensures that both employees and vendors receive only the access level needed to perform their assigned duties.

THE SECURELINK SOLUTION

A secure remote access platform will automate least-privileged access via granular controls and permissions. SecureLink meets this need and uses a Zero Trust approach, operating on the principle of “never trust - always verify” for each privileged access attempt. It also enables authorized users to adjust system access to eliminate bottlenecks. Changes can be made quickly, in batches, or at the individual user level.

PROTECT SYSTEMS, COMMUNICATION, AND INFORMATION INTEGRITY

This CJIS policy will help state and local government agencies ask and answer critical questions about their security and CJIS compliance, including:

- Is CJIS data secure on its way to and from the cloud?
- Has the agency adopted automated technology that detects attacks, monitors events, and identifies unauthorized users?
- Is the agency using data encryption?
- Have they implemented intrusion detection tools to check inbound and outbound communications for unauthorized/unusual activities?
- Remember that to be compliant, you must ensure your contractors are compliant

THE SECURELINK SOLUTION

Your third-party remote access management tool should allow users to manage controls and permissions for each third party with remote access. SecureLink enables your agency to control and easily elevate, downgrade, or eliminate third-party privileges as needed on an individual and vendor-wide basis.

[9] Multi-factor authentication for remote access is multi-faceted

Delegating remote access security

For agencies overwhelmed with ensuring that they're meeting the complexities of CJIS, there is support available. SecureLink is a single-platform, automated remote access tool that can support government cybersecurity and compliance by verifying, identifying, and managing each government third party accessing government networks. The next steps for state and local agencies are to:

- Assess current operations and infrastructure
- Choose a solution that supports CJIS requirements
- Remember that to be compliant, you must ensure your contractors are compliant

NOTE: For agencies wondering whether they have the resources to satisfy the complexities of CJIS, there is good news. While strained technology budgets may always be a reality for small public agencies, the federal government has initiated multiple grant programs to fund technical initiatives for state and local agencies. The current COVID-19 pandemic has seen agencies ranging from criminal justice and public safety to health and human services receiving significant funding.[10]

[10] CARES Act Funding and Technology: What State and Local Governments Need to Know

Need more information? Download our free CJIS Compliance Checklist and learn how SecureLink can streamline your auditing process for compliance with state and local government security policy regulations.

DOWNLOAD

About SecureLink

Headquartered in Austin, Texas, SecureLink is the leader in third-party security, providing secure third-party remote access for both highly regulated enterprise organizations and technology vendors. SecureLink solves and secures the greatest point of risk in the third-party lifecycle for more than 30,000 organizations worldwide, providing companies across multiple industries, including healthcare, manufacturing, government, legal, and gaming, with secure remote access with identity management, access controls, audit, and compliance assurance.

securelink.com | 888.897.4498 | contact@securelink.com