imprivata®

7 Considerations For Achieving CJIS Compliance

Expert Advice From Government Peers Who Have Successfully Complied With CJIS AA

This whitepaper explores what every agency needs to know in order to comply with the CJIS AA Security Policy. Most importantly, it provides 7 considerations from your peers, who have successfully achieved compliance at their own agencies.

TABLE OF CONTENTS

INTRODUCTION—CJIS AA SECURITY POLICY

The U.S. Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division now requires strong passwords and advanced authentication (AA) technology to secure access to CJIS information and systems. While law enforcement officials require near-instant access to information provided by CJIS, maintaining the security of this information is imperative to ensure that data is never accessed by unauthorized individuals.

Recognizing the competing objectives of timely access and strict security, the FBI has mandated compliance with the CJIS Security Policy, which provides requirements and guidelines for accessing CJIS information. This policy applies to every agency and individual with access to CJIS systems. Improper access of criminal justice information can result in administrative sanctions including termination of services and criminal penalties.

CJIS AA SECURITY POLICY REQUIREMENTS—WHAT YOU NEED TO KNOW

Key provisions of the CJIS Security Policy are focused on authentication and auditing. The main CJIS mandates specify that all law enforcement officials connecting to CJIS systems via wireless networks must use:

- Unique IDs and strong passwords by September 30, 2010
    - The CJIS Security Policy states that agencies must use unique IDs and strong passwords by September 30, 2010. Specifically, 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 Userid.
        - 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.
- Advanced authentication by September 30, 2013

WHAT IS ADVANCED AUTHENTICATION?

Advanced authentication (AA) provides additional security to accessing CJIS data by confirming the identity of a user beyond a username and password. In order to satisfy AA requirements, agencies must use two-factor authentication to authenticate users. Approved means of two-factor authentication include finger biometrics, smart cards and tokens. Regarding AA, the CJIS policy specifically states:

5.6.2.2 Advanced Authentication:

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

WHO IS ADVANCED AUTHENTICATION A REQUIREMENT FOR?

Advanced Authentication is a requirement for the following:

- All mobile systems, including laptops (removed from squad cars) and all mobile devices, such as cell phones and PDAs, that run National Crime Information Center (NCIC) access transactions
- Any device that uses the Internet, wireless, or dial-up connections to run or process NCIC transactions

WHAT IS CJIS' AUDITING REQUIREMENT?

The CJIS policy requires auditing to provide integrated reporting capabilities that track data access, network authentication, and application activity at the individual user level.

Log-on attempts, password changes, and other security-related events, must be securely logged as part of the agency's auditability and accountability controls. These requirements are detailed in Policies 5.6.2.1

Policy 5.4.1.1 - Auditable Events

The following events shall be logged:

- Successful and unsuccessful system log-on attempts.
- Successful and unsuccessful attempts to access, create, write, delete or change permission 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.

Imprivata OneSign streamlines the implementation of audit controls by tracking and consolidating the disparate employee access events outlined in the CJIS Security Policy. With Imprivata OneSign, agencies can rapidly respond to audit inquiries with real-time, aggregated views of when, how, and from where an employee gained network and application access. Imprivata OneSign reports show who is sharing passwords, what applications users are authorized to access, and what credentials they are using. When users leave the agency or are no longer authorized to access CJIS systems, Imprivata OneSign ensures that access—across all user accounts—is instantly revoked.

WHY COMPLY NOW?

Rather than waiting for the 2013 deadline, there are numerous advantages to complying with CJIS now. These include:

System Upgrade

Though a deadline of September 2013 may appear to provide plenty of time for organizations to meet the CJIS advanced authentication requirements, in practice it does not. Any agency considering or planning to acquire or upgrade a system that links to CJIS information must implement AA for that system as it is deployed—even if it is placed into service prior to 2013.

Auditing

Many of the CJIS authentication and auditing requirements are currently being mandated independently at the state and local levels. By implementing a solution to address these requirements now, agencies can simultaneously achieve CJIS compliance.

Grants and Funding

Grants and Funding are available for many agencies. As the 2013 deadline approaches, competition for funding at the local, state, and federal levels will increase dramatically. Grants and budget dollars available today may not be available as the cut-off date for compliance nears. Agencies are also implementing advanced authentication early to meet other state and local government mandates, or simply because it's a best practice.

Ultimately, unique IDs, strong passwords, advanced authentication, and audit controls are best practices that every organization should be planning to adopt. The FBI requires their use because they protect sensitive data. Implementing a solution now can help an organization avoid security breaches in the years and months before compliance is required.

7 CONSIDERATIONS FOR COMPLYING WITH CJIS AA

At times like these, you need expert advice—not from a vendor, but from actual peers who have successfully complied with CJIS at their own agencies—from those who have measured the results against the investment, and can share their experiences. So we approached some of our customers and asked them what advice they'd give to other agencies who are trying to comply with CJIS AA. What follows are 7 considerations for ensuring success based on their experiences.

1. CHOOSE A VENDOR THAT SUPPORTS ALL CJIS-APPROVED AUTHENTICATION METHODS

The CJIS Security Policy requires that AA requirements must be supported by the authorized authentication methods. These methods include smart cards, electronic token devices, paper/inert tokens and finger biometrics. Selecting the best form of two-factor authentication to implement will depend heavily on the specific needs of the organization. It's important to keep in mind that those needs can vary over time and across the organization, and deploying a solution with limited options will likely not serve all groups well.

2. CONSIDER HOW SECOND FACTOR AUTHENTICATION WILL AFFECT OFFICER WORKFLOWS

When choosing a solution, agencies must consider how implementing second factor authentication will effect officer workflows. In the fast-paced environment of law enforcement, it is imperative that second factor authentication does not disrupt officer workflows or productivity. Choose a solution that requires officers to only provide second factor authentication only once during their shift, and save time with a grace period.

3. EXAMINE WHETHER YOU NEED A VIRTUAL OR PHYSICAL APPLIANCE

The latest authentication software support both physical and virtual desktop environments. Consider whether or not your department is looking to move to a virtual desktop environment when evaluating solutions, or if your department prefers a physical, hardened appliance.

4. CONSIDER A SOLUTION THAT REQUIRES NO SCHEMA EXTENSIONS OR OTHER MODIFICATIONS TO EXISTING LDAP DIRECTORY

When an agency is under pressure to meet CJIS guidelines—either because it is upgrading a major system or to meet a state or federally-mandated deadline—the last thing it needs is to further disrupt the IT environment with changes to its directory or infrastructure. Choose a solution that fits easily into existing IT infrastructions in order not to disturb workflows.

5. ENSURE YOUR SOLUTION PROVIDES END-TO-END COMPLIANCE WITH THE FIPS 140-2 DATA ENCRYPTION STANDARD

CJIS requires FIPS 140-2 compliance for biometric systems and criminal justice information stored or transmitted outside physically secured locations. Ensure that the biometrics you choose comply with the FIPS 140-2 Standard.

6. CHOOSE A SINGLE PLATFORM SOLUTION THAT SUPPORTS CAPABILITIES FOR SELF-SERVICE RESET OF DIRECTORY PASSWORDS

Consider the effect of the new policy on law enforcement agents and the IT helpdesk. While it's relatively easy to mandate longer passwords that expire, personnel will have a more difficult time remembering passwords for each of the many applications they need to access. The result will be increased password reset requests to the helpdesk.

7. CHOOSE A SINGLE PLATFORM SOLUTION THAT SUPPORTS SINGLE SIGN-ON TO ALL APPLICATIONS

Consider a solution that also enables single sign-on to all applications. With single-sign on, agencies can profile an application's sign-on behaviors and enable application profiling without scripting or modification of application code.

IMPRIVATA ONESIGN®—A SIMPLE SOLUTION TO COMPLEX REQUIREMENTS

Imprivata OneSign® offers a simple solution to complex CJIS requirements that can be implemented today. Furthermore, it enables organizations to meet CJIS secuirty requirements while streamlining—rather than hindering—access to vital information for officers and reducing the workload on already overtaxed helpdesk and IT departments.

Beyond fulfilling the vital password, advanced authentication, and event auditing requirements of hte CJIS Security Policy, Imprivata OneSign offers a broad range of benefits to law enforcement, public safety, judicial, and probation/correctional organizations.

CONSIDERATION	IMPRIVATA ONESIGN
VENDOR SUPPORTS ALL CJIS-APPROVED AUTHENTICATION METHODS	Supports a wide range of CJIS-approved advanced authentication technologies: • ***Multiple card types*** – Supports active and passive proximity cards, Windows smart cards, building access cards, and government ID card technologies from leading vendors. • ***Finger biometrics*** – Supports fingerprint biometrics and works with readers embedded in laptops as well as USB readers that can be mixed and matched as needed on workstations. Because Imprivata OneSign is based on a centrally managed architecture, agents need enroll their fingerprint just once, no matter how many workstations they access. • ***Tokens*** – Includes a built-in RADIUS server to handle remote access authentication using DIGIPASS tokens by VASCO, RSA SecurID tokens, Secure Computing tokens, or passwords.
CONSIDER HOW SECOND FACTOR AUTHENTICATION WILL AFFECT OFFICER WORKFLOWS	Minimizes officer disruption by allowing officers to authenticate via 2 factor (i.e. password plus biometric swipe) at the start of their shift and "unlock" their workstation with a fingerprint alone.
VIRTUAL OR PHYSICAL APPLIANCE	Because it is designed for rapid enterprise deployment and easy integration, Imprivata OneSign's appliance-based solution can be implemented quickly and with minimal installation costs—key requirements for most organizations seeking CJIS compliance.
REQUIRES NO SCHEMA EXTENSIONS OR OTHER MODIFICATIONS TO EXISTING LDAP DIRECTORY	Requires no changes to user directories, applications, or physical access control systems, and does not require additional staffing or specialized management skills. The Imprivata OneSign platform is designed to fit easily into existing IT infrastructures and workflows, and is managed from a single, easy-to-use Web-based administrative console.

CONSIDERATION	IMPRIVATA ONESIGN
END-TO-END COMPLIANCE WITH THE FIPS 140-2 DATA ENCRYPTION STANDARD	Meets all Federal Information Processing Standards (FIPS) 140-2 encryption and data protection requirements.
SINGLE PLATFORM SUPPORTS CAPABILITIES FOR SELF-SERVICE RESET OF DIRECTORY PASSWORDS	Officers need to remember only one password, and with self-service password management, they can easily reset their own passwords without helpdesk intervention. Imprivata OneSign enables agencies to meet CJIS password management requirements while streamlining officer access to CJIS data, reducing the IT helpdesk burden, and automating the password change processes for all applications.
SINGLE PLATFORM SUPPORTS SINGLE SIGN-ON TO ALL APPLICATIONS	Enables single sign-on to all applications: CJIS, web, client-server, Java, and legacy terminal emulators. Using a simple, drag-and-drop interface, administrators can dynamically profile an application's sign-on behaviors, enabling rapid application profiling without scripting or modification of application code—and with no directory changes.

To learn more about Imprivata's solution for CJIS, please e-mail sales@imprivata.com with "CJIS" in the subject line, or visit our website at "www.imprivata.com".

Offices In:
Belgium • Germany
Italy • Singapore
UK • USA

1 877 ONESIGN
1 781 674 2700
www.imprivata.com

WP-CJIS-Ver1-09-2010