Unpacking CJIS MFA Requirements

Learn the Fundamentals to Get MFA Ready

Safeguarding sensitive information is a challenge that cuts across industries, but the stakes are especially high for law enforcement officials and agencies. The unauthorized access of data stored in incident reports and digital evidence can undermine criminal investigations, threaten reputations and put lives at risk.

That's why the FBI recently introduced more stringent requirements for authenticating users across different platforms and devices. Starting October 1, 2024, organizations that store and access criminal justice information (CJI) must implement multi-factor authentication (MFA) across all systems and applications. The goal: to prevent data breaches and make sure that information can only be accessed by individuals who are authorized to view it.

Yet there's no one-size-fits-all solution when it comes to complying with the new requirements. In this white paper, we'll review what's behind the mandate, what information you need to protect and how your organization can find the right path to CJIS compliance.

WHITE PAPER

What's at Stake With the CJIS Security Policy

From arrest records to digital evidence, CJI is hugely important to both criminal investigations — where, by one estimate, it factors in about 90% of the time — and ordinary public safety operations. It helps law enforcement officials make more accurate, efficient decisions in the administration of justice. It helps investigators identify patterns and streamline crime-solving strategies.

Mishandling CJI carries serious real-world consequences. Careers and reputations can be ruined; innocent people can be sent to jail while criminals walk free. Increasingly, public agencies must also protect CJI from malicious actors. In 2020, for example, hackers compromised the Cooke County Sheriff's Office in Texas, posting screenshots of alleged CJI. Other attacks have blocked access to investigative files and videos and knocked 911 services offline. Even when information isn't leaked to the public, it may not be admissible in court if prosecutors argue that the chain of custody has been compromised.

Failure to comply with the new CJIS requirements could lead to a denial of access to CJI data, in addition to monetary fines. That's why it's critical for agencies to maintain data integrity — and craft protocols that ensure both transparency and accountability whenever users access it. These protocols are at the heart of the new CJIS requirements.

Enter Multi-factor Authentication

The goal of any authentication mechanism is to allow only authorized users to access sensitive data — and keep all others out. Increasingly, it's clear that the way many agencies currently secure access to CJI falls short of that mandate.

In particular, most require nothing more than a username and password, in spite of mounting evidence that account information is dishearteningly easy to steal. In fact, 89% of organizations experienced a phishing attack in the past year aimed at compromising people's login details.

MFA strengthens security by requiring individuals to provide multiple authentication factors. In particular, users must authenticate their identities using at least two of the following:

- Something you know — e.g., Personal identification number (PIN) or security code
- Something you have — e.g., Smart cards, mobile devices, security keys or tokens
- Something you are — e.g., Fingerprints, facial scans, iris scans or other forms of biometric

CJIS Security Policies have evolved with time, but they now require all organizational users to employ MFA on all systems by October 1, 2024.

Understanding the MFA Landscape

Like many security technologies, MFA has evolved over time to keep up with changing threats and address different constraints and use cases. On the one hand, that means there's a wide variety of MFA methods and solutions on the market. On the other hand, it means that organizations must be mindful when selecting the best fit — especially since some methods are more secure than others.

Here's an overview of the most popular MFA methods put on a scale to identify the least to most secure approach.

< Least Secure ••••••••••••••••••••••• Most Secure >

Authentication Method	SMS or Voice Authentication	Push Authentication with Mobile App	OTP Authentication with Mobile App or Token	Phishing-resistant MFA
How it works	Users receive a one-time password or code via SMS or phone call, which they must enter to successfully log in.	Cryptographic techniques link a device to its owner's identity via a specialized app. Users then employ that device to approve or decline login requests.	Cryptographic techniques link a device to its owner's identity via a specialized app. Users then employ that device to receive a one-time password or code, which they enter to successfully log in.	Advanced cryptographic techniques based on PKI or FIDO standards are stored on a specific device, such as a card or USB security key, that's secured with an additional factor like a PIN or fingerprint. Users must present the device, card or token to successfully log in.
Weaknesses	**Phishing attacks** trick users into revealing their log-in details with malicious messages and links. **SS7 attacks** exploit security vulnerabilities in telephonic protocols to intercept voice and SMS communications. **SIM swapping** enables scammers to gain access to a user's phone by tricking the carrier into rerouting communications to a different device.	**Push bomb attacks** use compromised log-in credentials - for example, exposed corporate applications when a user leaves their desktop unattended - to trigger multiple log-in attempts. Users may grow frustrated with the repeated notifications and assume it's a technical error — or accidentally swipe "yes" and let the fraudsters into their account.	**Phishing attacks** are more difficult with app and token-based OTPs, but they are not impossible — especially with the rise of more sophisticated malware.	Phishing-resistant MFA represents the strongest authentication method in the market. Although users could be tricked into sharing their device, this would still require the user to cooperate in revealing the secret to use the credential for authentication.

HID

DID YOU KNOW?

CJIS Security Policy introduces the reference to **Authenticator Assurance Level 2 (AAL2)**, which offers a higher level of security but also comes with stricter specifications. Also referred to as **phishing-resistant MFA**, AAL2 requires individuals to present a physical authenticator that uses an additional factor (i.e., something they know, have or are) to unlock a secret that is stored in it. This could be:

- A physical authenticator and a memorized secret
  Example — a smart card or security key that's secured by a PIN
- A physical authenticator and a biometric that has been associated with it
  Example — a mobile device that's secured by a fingerprint

Organizations don't have to implement phishing-resistant MFA to comply with CJIS Security Policies; *it is only required for organizations that implement Personal Identity Verification - Interoperable (PIV-I) or Commercial Identity Verification (CIV) compliant credentials. However, HID strongly recommends it for strengthened security without much additonal expense or disruption to current operations.*

When Is MFA Required?

MFA is required whenever you use a device — whether agency issued or personal — to access CJI. For example, you'll need it to:

Authenticate any workstation that is connected to the same network as a CJI file repository or database

Authenticate any device that stores or could store CJI data*

Authenticate web applications or Software-as-a-Service (SaaS) that contain CJI**

Do I Need FIPS 140-2 Certification?

The CJIS Security Policy requires FIPS 140-2 certification only for federal government entities — or organizations that choose to implement FIPS 201 standards. However, as you look for MFA solutions, it's worth seeking vendors that comply with FIPS standards, as this indicates their adherence to state-of-the art security protocols.

* i.e., that contains an application that caches the data or could be used to download it
** Though device-level authentication with single sign-on (SSO) is often simpler

HID

Paths to MFA - And What They Look Like for Users

The best way to implement MFA will depend on each organization's budget, needs and the systems that are already in place. The goal: to select a flexible, user-friendly solution that safeguards data without standing in the way of critical law enforcement and administrative tasks.

Here are a few potential paths for law enforcement agencies to explore.

YOUR ID CARD AS A "KEY" TO ACCESS CJI

Organizations that already use smart cards can extend their utility by enrolling them in a software solution that associates each card with a unique PIN, password or biometric — and using them as an MFA factor when accessing digital systems and devices.

Pros
MFA capabilities can often be added to existing smart cards within a matter of days, enabling a single card to serve as visual identification and grant access to both physical and digital resources.

Cons
Maximum, phishing-resistant security can only be achieved with cards that are powered by PKI or FIDO technology.

What does it look like for users?
1. Present card or badge to a contactless reader (either already embedded in the device, or an external reader)
2. Enter PIN to authenticate

MOBILE DEVICES

Organizations can take advantage of devices that are almost always at hand by embedding them with cryptographically protected software tokens (aka authenticator apps) — and using them as an MFA factor when accessing other systems and devices.

Pros

Mobile MFA is among the most flexible solutions on the market, helping secure not just cloud applications but also mainframes, client and server log-ons, desktop client applications, VDI and VPN. Using a mobile device is convenient for law enforcement officials (they don't need to have a new device) and less costly for organizations.

Cons

Not all agencies provide personnel with corporate mobile devices. And though mobile MFA solutions do not store or record any personal data, users might be uncomfortable with using their own devices to authenticate.

What does it look like for users?

1. Enter log-in info
2. Use authenticator app on mobile phone to approve or deny the log-in request or receive an OTP code

USB SECURITY KEYS

USB keys that are powered by PKI or FIDO technology are fast, secure and easy to deploy, streamlining access to both digital and physical resources.

Pros

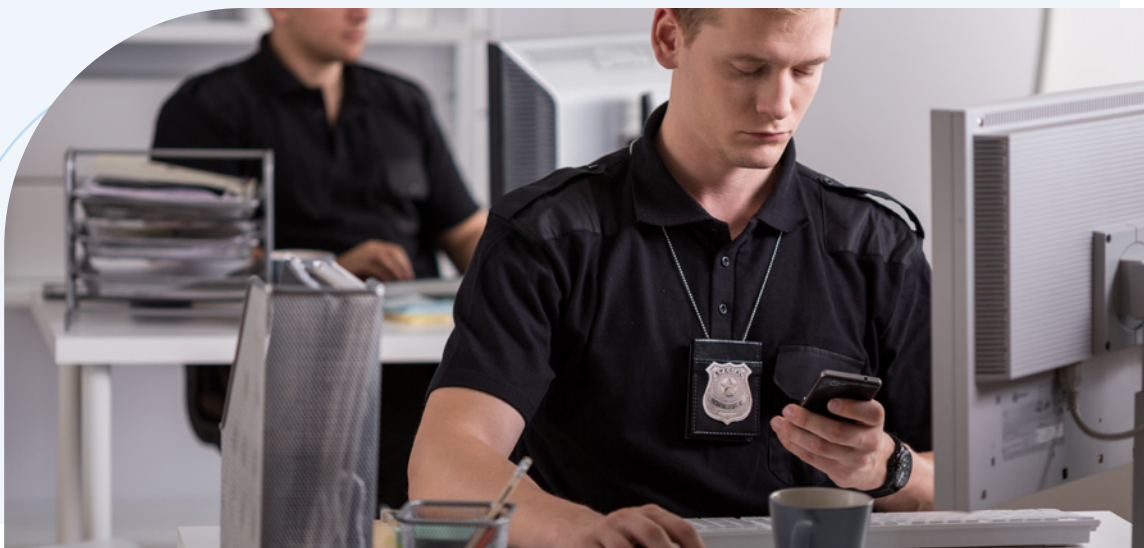
Security keys offer fast, flexible identity assurance in a variety of digital and physical contexts. They are convenient and unobtrusive and don't require additional reader hardware. Best-in-class solutions support FIDO and PKI standards for maximum phishing resistance.

Cons

Security keys tend to be less commonly used for physical access and, if a reader is not an option, they also depend on how many (and which) USB ports are available in users' devices.

What does it look like for users?

1. Insert USB security key into USB drive or a high-frequency reader – Near-Field Communication (NFC) – either embedded in the device or external
2. Enter PIN or biometric factor to authenticate



HID

Selecting Your Path to MFA: Four Questions to Guide Your Decision

It can be daunting to navigate the constraints and considerations involved with selecting the MFA path that best fits your needs. Given the impending deadline, some organizations may prefer to focus on speed and efficiency. Of course, solutions that can scale to fit changing requirements may be more cost-effective in the long term.

HID is a worldwide leader in trusted identity solutions, and we've helped several state and local agencies navigate CJIS Security Policies. We've put together four key questions to help guide your decision:

1. What infrastructure is already in place and what investments are you able to make?
Many software-based solutions can support the authentication methods and form factors you already have in use, from smart cards to mobile devices. However, to maximize security in the long run, you'll need a factor that can support PKI or FIDO technology.

2. What type of personnel must you support?
Field officers are always on the move; their solutions must be fast, flexible and user-friendly. Justice department officials, meanwhile, may need to maintain an audit trail that logs where they are and what type of information they've accessed.

3. What other regulations is your organization subject to?
For example, federal government entities — and those that choose to implement FIPS-201 standards — must select a solution that's certified compliant with FIPS-140-2.

4. When do I need to be MFA ready to meet the deadline?
There is a pre-audit, audit and post-audit process. According to the (CJIS) Audit Unit (CAU), the first communication with the main contact from an agency starts six months before the scheduled audit.

Law enforcement officials and agencies operate in high-pressure environments where every minute counts. They expect security solutions that power their work with confidence and ease. Fortunately, with attention and planning, agencies can implement MFA solutions that keep CJI secure — while safeguarding their personnel and the public that they serve.

Still struggling with CJIS? To get the answers you need, check out the following resources or contact one of HID's security experts:

Blog Post – The Top 5 Questions About MFA for CJIS
Case Study – The Columbia County Sheriff's Office
Case Study – Phoenix Police Department

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here

2024-01-05-iams-unpacking-cjis-mfa-requirements-wp-cs-en PLT-07554
Part of ASSA ABLOY