AXIAD

Complying with CJIS MFA Requirements

Who should read this? Enterprise identity architects, CISOs, IAM program leaders, and audit and compliance analysts for organizations that rely on Criminal Justice Information Services (CJIS) data.

What they'll learn: New CJIS requirements, timelines, how to address the needed changes, and how readers can benefit from an approach that adds strong MFA credentials to existing systems.

It's possible that no public organization is a better example of the dramatic changes wrought by "digital transformation" than the FBI's Criminal Justice Information Services (CJIS)[2]. What started in 1924 as a small FBI division that collected and catalogued fingerprints has become, on its one hundredth birthday, one of the most all-encompassing, complex, and critical law enforcement tools of the modern era.

CJIS is now responsible for providing programs like:

- National Crime Information Center (NCIC and NCIC2000)
- National Instant Crime (NIC) background check
- Uniform Crime Reporting (UCR)
- Integrated Automated Fingerprint Identification System (IAFIS)
- National Incident-Based Reporting System (NIBRS)
- Bioterrorism Risk Assessment Group
- Law Enforcement Records Management Systems (RMSs)

EXECUTIVE SUMMARY

- By October 1, 2024, any organization that accesses the FBI Criminal Justice Information Sytems (CJIS) must use multifactor authentication (MFA)
- This includes all state, county, and local police forces as well as justice departments and legal teams
- By CJIS definition the MFA solution must meet NIST AAL2 standards
- The AAL2/3 standard recommends the use of either FIDO or PKI credentials (or both) to achieve phishing-resistance
- The CJIS policy itself states the need for "Acceptance of PIV Credentials (PKI credentials), from both Organizational and Non-Organizational Users"[1]
- The good news: these credentials and the security they provide can be added to many existing MFA implementations

[1] CJIS Security Policy Resource Center
[2] Criminal Justice Information Services (CJIS)

PROTECTING VITAL DATA

Within the US alone, every state, regional, county, and local law enforcement organization participates in an interchange of data with CJIS, providing new inputs and pulling in the data that helps solve crimes.

While Law Enforcement's dependence on this data has gone up, adversaries have aggressively targeted their systems to slow them down, lock them up, or hold them for ransom. A few examples:

- In May of 2023 the Dallas Police Department suffered a ransomware attack by the Royal group that affected critical services and more than 30,000 accounts in 40 departments across 17 systems. It also exposed 1.2 TB of data and credentials[3].
- In a prime example of a "digital feeding frenzy", the October 2023 loss likely led to a July 2024 announcement from Dallas County that another group – the Play ransomware group– had exposed data for more than 200,000 people nationwide including social security numbers, medical information, health insurance details, and other data[4].
- And this is trend is clearly not isolated to Texas: in January of 2024 the Center for Internet Security (CIS) reported that malware attacks on government departments and agencies had increased by 148%, that government-targeted ransomware incidents were 51% more prominent during the first eight months of 2023 over the same times in 2022, and that direct non-malware aided cyberattacks on these targets increased by 37%[5].
- The CIS report states that these attacks resulted in a 313% rise in endpoint security services incidents like data breaches, unauthorized access and insider threats.

[3] Ransomware attack on City of Dallas knocks police website offline
[4] Dallas Ransomware Attack Exposed Info for 200,000 People
[5] Cyberattacks on state and local governments rose in 2023, says CIS report

CJIS, as the nerve center of law enforcement and government information, saw these trends in 2022 as a clear and present danger: they moved to strengthen systems and increase robustness wherever their data was required.

CJIS SECURITY POLICY UPDATED

The latest version of the CJIS security policy – version 5.9.5 – includes revisions that affect all entities who have access to CJIS data, including education departments, police, interagency teams, technology vendors and more. An article in Government Technology states these changes make the policy "roughly 50% new[6]."

Part of the policy's "newness" was an insistence on multifactor authentication (MFA) across all systems and applications that store and access Criminal Justice Information (CJI). MFA as a principle recognizes that password-heavy authentication systems – let alone password-only systems – are a non-starter for strong authentication and access controls. MFA requires the use of multiple factors for every authentication attempt, including:

- Something you know, like passwords, PINs, or security codes
- Something you have or possess, like smart cards, mobile devices, security keys, or tokens
- Something you inherently "are", represented by fingerprints, facial scans, iris scans, or other biometric tools

Starting October 1, 2024, organizations that store and access CJI must have implemented MFA using at least two of those factors to authenticate sessions across all their systems and applications. Failure to comply with this requirement could lead to a denial of access to CJIS resources and data, which could be crippling for even the smallest of local police forces. (A list of requirements in the CJIS policy that explicitly refer to MFA is in this briefs' end notes[7].)

The new CJIS policy also includes "prescriptive teeth" that define how MFA should be achieved. Unfortunately, it's not as direct a reference as it could be, as the CJIS policy points to another standard, the National Institute of Standards and Technology's (NIST) four-volume regulation called SP 800-63 governing Digital Identity Guidelines[8].

Volume B of SP 800-63 covers "Authentication and Lifecycle Management" and spells out prescriptive details for achieving MFA. Some practitioners and auditors who've been focused only on the verbatim CJIS policies have already been caught flat-footed by this document's requirements for "phishing-resistant MFA."

[6] FBI Revamps Criminal Justice Data Security Policy

[7] See these CJIS sections: 5.5 Access Control; 5.6 Identification and Authentication; 5.10 Systems and Communication Protection; 5.14 System and Services Acquisition; 5.18 Contingency Planning

[8] Digital Identity Guidelines

PHISHING-RESISTANT MFA, ACCORDING TO NIST

MFA solutions as defined in the previous section – those incorporating something you *know*, something you *have*, and something you *are* – have been around since 2016 or so. Why have they not stopped the flood of government attacks? In part because MFA has not been mandated, but also because authentication factors are not created equal. There is a significant difference between passwords that can be stolen and then purchased for a few dollars per hundred (as in the Dallas County case), versus strong certificate-based or FIDO-based credentials.

NIST SP 800-63 is the seminal document that defines the level of assurance required for different authenticators and authentication mechanisms. "Level of assurance" describes the degree of certainty that a credential used for authentication is legitimate and correctly refers to the identity of the person using it. The new CJIS policy points to this document for assurance standards; and these standards, in turn, point to NSTS's 800-63B Authenticator Assurance Level 2 (AAL2) as a requirement. SP800-63B strongly recommends that when using MFA, AAL2 be achieved by using a combination of cryptographic devices and cryptographic software:

> "A multi-factor cryptographic device is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key."

In NIST's explanation for AAL2 they say, "The multi-factor cryptographic device is something you have, and it shall be activated by either something you know or something you are." This is also called "phishing-resistant" MFA because it provides security against widespread phishing attacks that have been so successful because of the en masse harvesting of knowledge factors like passwords, passphrases, and PINs.

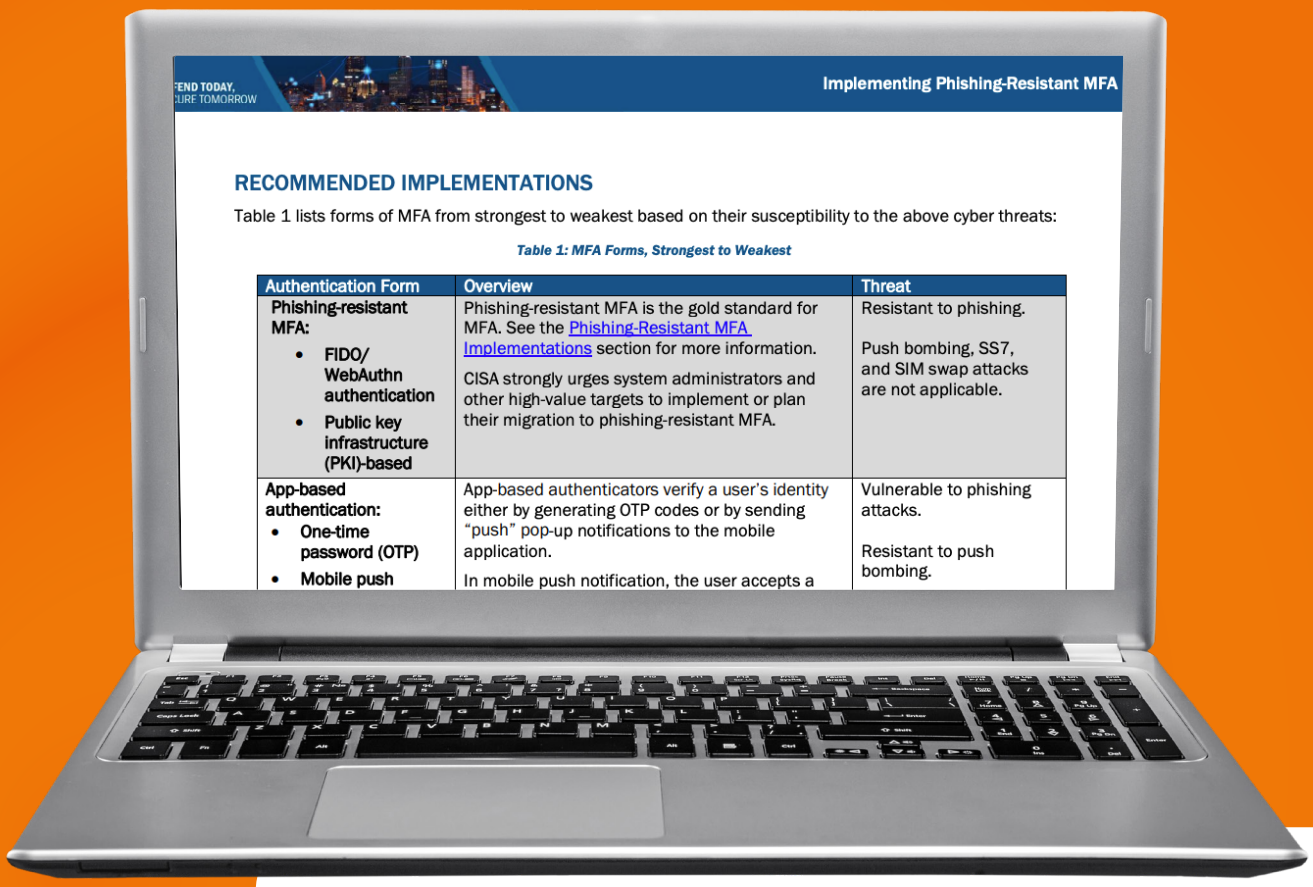
NIST isn't alone in recognizing the need for phishing-resistant MFA. The US Cybersecurity and Infrastructure Security Agency (CISA) has a web page devoted to defining "phishing-resistant MFA[9]" In this document CISA recommends that a broad swath of earlier forms of MFA – like SMS-based authentication, voice-based systems, push notifications, one-time passwords and one-time tokens – be discontinued. Instead, practitioners should upgrade these systems in favor of two far stronger, well-known methods: PKI and FIDO.

[9] Implementing Phishing-Resistant MFA

PHISHING-RESISTANT MFA, ACCORDING TO NIST

CONTINUED

A screen shot from CISA's current guidance on how to implement phishing-resistant, next-generation multifactor authentication.



While the CJIS policy points to NIST and SP 800-63 as key reference, it does contain its own unique requirements for authentication's process and strength:

- CJIS 5.6: IA-5.n(9) "At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators…"
- CJIS 5.6: IA-5.(k 2) "…the ability to revoke or suspend the authenticator".

Solution architects who design these systems (and the auditors who verify them) should keep both documents in mind as they ideate and evaluate their strong MFA.

STRONG CJIS AUTHENTICATION USING PKI AND FIDO

Public key infrastructure, or PKI, has been around as long as the internet. PKI is the "set of roles, policies, hardware, software and procedures" that "create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption[10]." PKI is the complex system that merges TLS certificates, certificate authorities, web addresses, and devices into a secure and trusted relationship. CISA says "PKI-based MFA comes in a variety of forms; a well-known form of PKI-based MFA is the smart cards that government agencies use to authenticate users to their computers. PKI-based MFA provides strong security and is sensible for large and complex organizations."

As complex and confusing as PKI can be, it is also well-known and widely trusted. The process for creating and managing public and private certificates – called "transport layer" (TLS) or "secure socket layer" (SSL) certificates but all based on the X.509 standard[11] – has allowed the internet to support over 302 million certificates as of January 14, 2024[12]. Most enterprises have some sort of PKI solution in place to manage their web properties, domain names, email and machine-to-machine connections. (Many, however, don't want to be PKI specialists or manage their own PKI: see the sidebar on PKI-as-a-Service.)

When used in conjunction with an MFA solution, PKI-based MFA can be applied to the smart cards that government agencies use to authenticate users to their computers. It can be applied to hardware-based authenticators like those made by Yubico, Thales and IDEMIA. PKI certificates can even be applied to dedicated end user devices, which is the technology behind email signing and device-based authentication.

As the CISA guidance states, "PKI-based MFA provides strong security and is sensible for large and complex organizations."

Passwordless FIDO passkeys represent another, different form of public key infrastructure. They are managed by the WebAuthn protocol and published by the World Wide Web Consortium (W3C). WebAuthn support is included in major browsers, operating systems, and smart phones. WebAuthn works with the related FIDO2 standard to provide a phishing-resistant authenticator.

Perhaps the most important thing to remember about FIDO is that it's not supported everywhere: there are systems and platforms and browsers that do not yet support advanced FIDO or WebAuthn standards. Many of the legacy systems used for authentication into large and small government agencies do not yet support FIDO. For this reason, most successful implementations of strong MFA use both FIDO- and PKI-based solutions.

[10] Public Key Infrastructure
[11] X.509 Public Key Certificate
[12] 11+ Latest SSL/TLS Certificates Statistics November 2024

DON'T RIP AND REPLACE: HOW AXIAD SOLVES FOR CJIS REQUIREMENTS

Upgrading CJIJS policy standards in light of unremitting, constant attacks is objectively a good thing. But most of the organizations governed by CJIS – from state and country law enforcement to local police forces and legal firms – already have some form of MFA in place.

Are those departments and agencies expected to rip and replace their authentication systems? Many IAM vendors would say Yes. But there is another way: Axiad Conductor.

Authentication systems have evolved from monolithic one-size-fits-all solutions to dynamic, service-based solutions. These solutions can combine one or more technologies with an ecosystem of products that include identity providers (IDPs), privileged access controls (PAM), machine-based identities like X.509 certificates, and hardware-based authenticators. In doing so they can come in alongside most leading IAM solutions, like Ping, Okta, or Microsoft, and provide exponential value without incurring significant overhead in either cost or manpower.

Axiad Conductor provides an advanced authentication toolset that combines the technologies needed to enhance existing multifactor authentication, with cloud-based PKI and robust credential management utilizing x.509 certificates and FIDO passkeys. It helps organizations deploy and manage strong authentication processes across people, machines and applications without replacing existing systems.

Axiad Conductor customers use any combination of physical authenticators – like smart cards, digital tokens, phone-based MFA, and hardware-based authenticators – and combines them with PKI-based or FIDO2-based credentials. The result is better phishing-resistant MFA that meets tough CJIS requirements with lower cost, happier end users, and fewer support calls.

To learn more about Axiad Conductor, download the product brief. Or you can call and speak to an integration expert who understand CJIS requirements and schedule a demo.

Axiad's PKI-as-a-Service

PKI has been the standard for machine-to-machine authentication for decades: it connects web servers to end users, browsers to clients, and devices to systems and services. But cybersecurity needs are ever-increasing, and some teams have had to short-staff their PKI groups to meet other security needs. And PKI requires no small amount of expertise and specialized knowledge.

Axiad Conductor can deliver Axiad PKI-as-a-Service: a consolidated, highly customizable, and scalable PKI solution that provides the digital trust your organization needs to transparently secure end users, devices, emails, attached documents and all the connections between these points.

The combination of product functionality and a true SaaS delivery model lowers the cost of operating in-house PKI and allows organizations to consolidate or retire costly or aging PKI systems. For more detail, visit PKI as a Service.