Solution guide

Cisco public

Meeting the FBI CJIS Security Requirements with Cisco Duo

The Criminal Justice Information Services (CJIS) Division of the US Federal Bureau of Investigation (FBI) allows state, local, and federal law enforcement and criminal justice agencies access to criminal justice information, provided agencies comply with CJIS security policy.

This quick guide will help you understand how Cisco Duo can help your law enforcement agency meet the newly announced MFA requirements outlined in the CJIS Security Policy.

The Scope of the CJIS Security Policy

The CJIS Security Policy applies to all entities with access to, or who operate in support of the FBI CJIS Division's services and information. The security policy is a collection of guidelines designed to safeguard criminal justice information (CJI)[1]. It provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Criminal justice agencies (CJA)[2] throughout the United States, including at the state, local, and national levels must comply with the CJIS Security Policy. Noncriminal Justice Agencies (NCJA)[3] must also comply and meet the minimum standard of security requirements to ensure the continuity of information protection. As law enforcement agencies acquire perpetually evolving mobile technologies, the risk of unauthorized access to CJI data increases. Consequently, fast and simple access to this data is critical, but there needs to be a balance of security and user convenience.

[1] CJI data is described in detail in section 4.1 of the CJIS Security policy.

[2] A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal inspectors General Offices are included.

[3] A NCJA is defined (for the purpose of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

Preparing for the FBI CJIS Security Policy MFA Mandate

In preparation for the October 2024 mandate to use multi-factor authentication (MFA) for accessing all CJI data, we recommend law enforcement agencies take the following steps:

1. **Understand MFA.** Educate your teams on what MFA is and how it works. MFA requires users to provide at least two forms of verification to access sensitive data, which increases the security of the system.

2. **Conduct an inventory and risk assessment.** Conduct an inventory of all systems, applications, and data that will require MFA. Determine the current access control methods in use and identify any gaps that need to be addressed to comply with MFA requirements.

3. **Foster vendor collaboration.** Collaborate with vendors to understand their MFA solutions. Ensure that these solutions comply with the CJIS Security Policy and can integrate with the existing infrastructure.

4. **Develop an implementation plan.** Document the deployment in detail including timeline, milestones, resources needed, roles and responsibilities, and budget. Remember to include plans for testing the MFA solution before full implementation. Cisco offers strategic security services to assist teams in planning and implementing transformational security programs like zero trust.

5. **Conduct user training.** Train all users on how to use MFA when accessing CJI. Include both technical training on how the MFA system works, as well as policy training on when and why to use MFA.

6. **Begin functional testing.** Conduct comprehensive testing of the MFA solution to ensure it works correctly and does not disrupt operations, including testing the solution's ability to withstand targeted cyber-attacks.

7. **Start the rollout.** Gradually roll out the MFA solution across the organization, prioritizing the most used applications.

8. **Monitor and adjust policy.** Once the MFA is implemented, continuously monitor its effectiveness and make necessary adjustments. Add regular audits to ensure compliance with the CJIS Security Policy.

9. **Document everything.** Keep thorough documentation of all processes, implementations, and trainings. In addition to demonstrating compliance with the mandate, a paper trail can be a useful reference for any future audits and policy updates.

Pro-tip: Duo offers a wealth of MFA documentation to assist agencies in deploying MFA to protect CJI data and the applications hosting it.

CJIS MFA Requirements: **Top 3 Facts**

1. MFA is a mechanism to verify a person's identity by requiring more than just a username and password but instead two or more of the following::
   - Something the user knows – password, passphrase, PIN.
   - Something the user has – a physical token, a device-based authenticator.
   - Something the user is – biometric authenticators (e.g., FIDO2-compliant)
2. MFA will be required when accessing a CJI system, device, app, or network. Authentication may occur via multi-factor authentication or a combination of two single-factor authenticators.
3. There are nine different authenticator types recognized by the CJIS Security Policy.
   - Acceptable MFA authenticator factors include a multi-factor one-time-password (OTP) device, multi-factor cryptographic software, multi-factor cryptographic device, and biometric authentication.
   - Single-factor options include combining one of the following with a memorized secret: look-up secret, out-of-band device, single-factor one-time-password (OTP), single-factor cryptographic software; and a single-factor cryptographic device.

The challenge

Law enforcement officers and their teams are on the front lines of protecting the public. As officers perform their mission-critical activities, the technologies designed to secure access to CJI data must not interfere with their tasks or fail to protect data privacy.

It is critical to balance security and user productivity by verifying device trust in a manner that is easy for IT to manage and does not disrupt mission or employee workflows. Organizations of all sizes must be able to seamlessly incorporate MFA into their IT security strategy while delivering the best possible user experience with minimal administrative overhead and a low cost of ownership.

IT teams throughout the law enforcement community seek solutions that can be deployed quickly, follow recommended best practices, align with compliance requirements, and make it easy for officers and their staff to adopt in their daily activities.

The solution

Duo provides organizations with best-in-class security technology and a trusted partnership to help build and maintain a well-rounded security program. We believe that by focusing on security fundamentals and best practices, you can easily achieve compliance with a variety of regulatory requirements and standards – beyond CJIS.

Key features

Deploy strong, phishing-resistant multi-factor authentication. Protect against MFA push fatigue and other social engineering attacks.

Secure CJI data against dodgy devices. Verify the security health and management status of endpoints *before* granting access to applications that house sensitive data.

Block untrusted devices. Auto-deny MFA access to unknown devices and define trust for each endpoint, whether managed or unmanaged, agency-issued, contractor-owned, or personal.

Maintain device hygiene. Prompt agency staff to update their OS patch levels and browser versions, and continually check for presence of device certificates, enterprise antivirus (AV) agents, disk encryption, and more.

Enforce least privilege access. Protect private apps and streamline officer access to just the apps they need with Passwordless Single Sign-on (SSO) and ZTNA, VPN-less access. This enforces the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.

Secure access to CJI data by frustrating threat actors, not users

Duo offers different editions to provide flexible solutions for agencies to easily address the CJIS MFA requirements. Duo's secure, easy-to-use approach enables rapid deployment and adoption of zero trust security for user access.

Duo for State and Local Law Enforcement

Duo offers different editions to provide flexible solutions for agencies to easily address the CJIS MFA requirements. Duo's secure, easy-to-use approach enables rapid deployment and adoption of zero trust[4] security for user access.

Along with being offered on FedRAMP, Duo is also officially listed on the StateRAMP Authorized Product List. StateRAMP represents the shared interests of state and local governments, third party assessment organizations, and service providers with IaaS, SaaS, and PaaS solutions — giving governments and procurement officials confidence in their service provider's data security capabilities.

Table 1. How Duo Editions Help

	Duo Essentials	Duo Advantage	Duo Premier
CJIS Criminal Justice Information Services Section: 5.5.6, 5.6, 5.6.2, 5.13.4.1, 5.13.7, 5.13.7.2, 5.13.7.3	• Supports multiple ways to authenticate • Provides automated management of authentication methods • Offers methods for users to report fraudulent access attempts • Can block unmanaged or unknown devices via Trusted Endpoints policy	• Includes everything from Duo Essentials • Enforces adaptive authentication techniques (e.g., identifies user behavior that falls out of typical norms) • Controls access to systems and applications with a secure log-on procedure, where required by the access control policy • Ensures end users have up-to-date security patches on their devices • Provides guidance for self-service remediation for systems that are out of date	• Includes everything from Duo Advantage • Offers secure, VPN-less access to private applications that house CJIS data to ease compliance with new MFA requirements • Detects and enforces presence of an MDM client or endpoint security agent prior to giving access

[4] Cisco believes there are four essential zero trust functions: establish trust, enforce trust-based access, continually verify trust, and respond to change in trust. Read more here.

Duo for Federal Law Enforcement Agencies (FedRAMP Certified Editions)

Duo offers different editions to provide flexible solutions for agencies to easily address the CJIS MFA requirements. Duo's secure, easy-to-use approach enables rapid deployment and adoption of zero trust security for user access.

Table 2. How Duo Editions Help

	Duo Federal MFA	Duo Premier
Products from Duo Security follow guidance as provided by NIST in attempts to comply with 800-53 and 800-63 Federal Edition has achieved **FedRAMP** level: **Moderate National Institute of Standards and Technology (NIST) 800-171 Rev2 SP 800-63** B Guidance NIST 800-53 Control: IA2, IA3, IA5, IA6, MA4, SC7, SC11. 800-63 Control: AL2 AL3 NIST 800-171 Control: 3.1.1, 3.1.2, 3.1.8, 3.1.11, 3.1.12, 3.1.14, 3.1.15, 3.1.18, 3.1.20, 3.3.1, 3.3.2, 3.3.8, 3.4.2, 3.5.2, 3.5.3, 3.5.7, 3.7.5 Authenticator Assurance Level (AAL) 2	Uniquely identifies and authenticates users Meets NIST digital identity guidelines Limits system access to authorized users Provides inventory of all endpoints accessing protected applications Provides local access protections online/ offline for DFARS requirements	Includes everything from Federal MFA Limits applications that authorized users are permitted to access Grants access only to healthy and compliant devices Adds a layer of authentication for privileged accounts Provides Asset Management, Risk Assessment, Access Control, Data Security, Protective Technology, and Continuous Monitoring
CJIS Criminal Justice Information Services Version 5.9 Section: 5.5.6, 5.6, 5.6.2, 5.13.4.1, 5.13.7, 5.13.7.2, 5.13.7.3 *Can also be achieved with non-FedRAMP editions	Supports multiple ways to authenticate Provides automated management of authentication methods Offers methods for users to report fraudulent access attempts	Meets the MFA requirements for PAM, general users, device policy etc. Ensures end users have up-to-date security patches on their devices Provides guidance for self-service remediation for systems that are out of date Can block unmanaged or unknown devices via Trusted Endpoints policy
FIPS 140-2 and FIPS 140-3 Federal Information Processing Standards Control: 1402 lv13	Is FIPS compliant with validated cryptographic modules in the Federal Editions • Zero-touch implementation for FIPS 140-2 and FIPS 140-3 compliant mobile authentication; no configuration required by administrators	

Solution guide

Cisco public

This resource highlights how Duo's editions address specific areas within the various frameworks, compliance requirements, and data privacy guidelines. Duo should be considered an integral component within overarching security strategies with its agnostic approach. It integrates with and complements other key security solutions in the market to empower organizations to meet compliance requirements.

Cisco Duo protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. A trusted partner to more than 40,000 customers globally, Duo quickly enables strong security while also improving user productivity.

Sign up for a free trial at **duo.com**.