Barkrum

SERVICE OVERVIEW

CJIS Readiness Assessment

The audit clock is already running. We help you meet it.

Every agency that touches criminal justice information is required to meet the FBI CJIS Security Policy, and that policy has just gone through its largest change in over a decade. Version 6.0 reorganized the entire standard around twenty policy areas mapped to the NIST 800-53 control families, and version 6.1 continues it on a new cycle of updates every six to twelve months.

> **CJIS Security Policy, current version 6.1:** *multifactor authentication and other Priority 1 controls are already sanctionable, formal auditing under the new policy is underway, and full compliance across all remaining controls is required by September 30, 2027.*

WHAT THE ASSESSMENT DELIVERS

Area	What it covers
Gap Assessment	Your current posture measured against the current CJIS Security Policy, the recommended first step before any remediation begins.
Control Mapping	Findings organized by the twenty policy areas and their underlying NIST 800-53 controls, prioritized by the policy's own P1 through P4 tiers.
Technical & Physical	Access control and multifactor authentication, audit logging, encryption, and the physical protections at every location where criminal justice information is handled.
Remediation Roadmap	A practical, sequenced plan that puts the sanctionable items first and the 2027 requirements on a realistic timeline.

THE BARKRUM DIFFERENCE

- **Led by a Certified Information Systems Auditor.** The assessment is performed by a practitioner holding the CISA credential, providing the independent audit authority a self assessment cannot supply.
- **Grounded in the frameworks behind the policy.** The assessment maps directly to the NIST 800-53 control families that CJIS v6.0 and 6.1 are built on, so findings speak the same language as the standard your agency is measured against.
- **Every location and system assessed directly.** Including the legacy applications and portals that touch criminal justice information, which are exactly where audits most often find gaps.
- **Built for both standards.** Mapped to the current policy your agency must fully meet by 2027, while accounting for the version audits are conducted against during the transition.
- **Fixed scope and fixed fee.** A defined deliverable on a defined timeline, built to withstand a review by your state CJIS Systems Agency.

WHY IT MATTERS NOW

This is no longer a distant deadline. Auditing under the new policy has already begun, multifactor authentication is already sanctionable, and the move to updates every six to twelve months means compliance is now an ongoing obligation rather than a one time project. Agencies that start with a gap assessment today give themselves a realistic runway to 2027, and a clear record that they acted in good faith.

Start with a Gap Assessment

Know exactly where your agency stands against the current policy, with a clear roadmap to the 2027 deadline. A fixed scope and fixed fee, delivered after a brief scoping conversation.

www.Barkrum.com