CJIS Posture Statement

Why ScamZero is outside the scope of the CJIS Security Policy

Version: 1.0 **Date:** August 2026

✓ Summary

ScamZero receives no Criminal Justice Information, connects to no criminal justice system, and is not a channel for reporting a crime.

No CJIS Security Addendum is required, and no personnel handling ScamZero data require CJIS clearance, because no such data reaches ScamZero.

1. What a Scam Safety Center Is

A Safety Center is a public-facing educational website branded for your department. A resident can paste a suspicious message into it and receive guidance on what to look for and what to do next. It is a prevention tool, not an intake system.

2. What ScamZero Does Not Touch

- ✓ No Criminal History Record Information (CHRI)
- ✓ No NCIC, III, NLETS or state CJIS system connection of any kind
- ✓ No CAD or RMS integration, and no read or write access to any department system of record
- ✓ No case, incident, arrest, citation or booking data
- ✓ No sworn-personnel personally identifiable information
- ✓ No biometric, fingerprint or photographic identification data

ScamZero requires no connection to your network, installs no software, and has no account on any department system.

3. Why Criminal Justice Information Cannot Enter the Product

A resident submits to **ScamZero**, not to your department. Your department never receives the submission, never receives the resident's identity, and never receives a result. That is a deliberate design decision, and it is what keeps this service outside CJIS scope in both directions.

The Safety Center states plainly that it is not a way to report a crime, and directs a resident who needs to file a report to the department's own non-emergency line and to federal reporting channels. Emergencies are directed to 911.

Because submitted content is never written to storage and the assessment is deleted on first view, there is also no retained body of resident material that could later be characterized as investigative.

4. How ScamZero States This

ScamZero does not describe itself as “CJIS compliant,” and you should be wary of any vendor that does. There is no FBI certification program for vendors and no accredited assessor pool — both AWS and Microsoft say so plainly in their own published guidance. Agencies are audited; vendors are not.

What ScamZero offers instead is a scoping determination you can file: the CJIS Security Policy defines Criminal Justice Information as the data the FBI CJIS Division provides, and applies to entities that access, process, store or transmit it. No FBI or state CJIS system supplies anything to a Safety Center, so no CJI is created, viewed, transmitted or stored at any point.

If your policy requires a signed CJIS Security Addendum regardless, ScamZero will sign it. It costs nothing and it closes the question. What ScamZero will not do is offer fingerprint-based background checks, because the authority to run them attaches to unescorted access to unencrypted CJI — access nobody here has.

Note also that a FedRAMP, StateRAMP or SOC 2 authorization is not a substitute for a CJIS scoping determination, and the policy says as much. ScamZero offers its security documentation as a general assurance, not as a CJIS answer.

> **If your agency reaches a different conclusion**
>
> Terminal Agency Coordinators apply their state's interpretation, and those differ. If your agency determines that a CJIS Security Addendum or additional documentation is warranted, contact support@scamzero.com and ScamZero will work through it with you rather than asking you to accept this statement as the final word.