How does Cyber Crucible serve law-enforcement and CJIS environments?

Short answer: Cyber Crucible fits Criminal Justice Information Services (CJIS) environments because it processes data locally, never collects criminal justice information (CJI), and can run on-premises or air-gapped inside the agency boundary. US data is handled by US-based personnel, which supports the CJIS Security Policy's personnel and data-handling expectations.

Why the architecture fits

- **CJI stays in the boundary.** No customer content is collected; analysis is on the endpoint, so CJI is not transferred to a third-party cloud.
- **US personnel for US data.** Offshore contractors do not handle US data or develop the agents.
- **Encryption and access control.** Strong authentication, role-based access, and encryption support the policy's technical controls.

The honest boundary

The CJIS Security Policy is enforced by the agency and its state CJIS Systems Agency; Cyber Crucible supports several of its control areas but is not itself a CJIS "certification." Personnel-screening and control detail is available under NDA.

Revision #2
Created 2026-07-23 15:18:28 UTC by Dennis Underwood
Updated 2026-07-23 18:19:58 UTC by Dennis Underwood