CJIS COMPLIANCE

70 Pages of Requirements. One Credential. Done.

How NextgenID helped First Advantage Biometrics turn the FBI's CJIS security policy requirements into a single audit reference

CHALLENGE:
When FBI Channeling Is the Business, Compliance Is Mandatory

As an FBI approved channeler, First Advantage Biometrics understands that failing a Criminal Justice Information System (CJIS) audit can have serious implications. When the FBI aligned its CJIS Security Policy with NIST 800-53 and introduced enhanced Identity and Authentication (IA) requirements, the channeler needed a solution that was technically sound, operationally practical, and audit-defensible, all without building an extensive inhouse Credential Service Provider (CSP) solution.

Three factors complicated the path forward:

A multi-page compliance requirement: The IA section includes an extensive IA control set aligned to NIST SP 800-53 Moderate. Line-by-line adherence would require extensive compliance documentation and associated resources to internally-audit and maintain it.

A segregated operating environment: The channeling CJI infrastructure is completely segregated from all other networks and communicates only with the FBI, precluding any external network or cloud-based biometric verification. The solution required a custom Match on Card approach to use on-PIV-I card biometric data verification. The PIV-I credential offers the best solution due to its status as a federally-approved multi-factor cryptographic device capable of storing multiple biometrics for unique identification and authentication of an individual prior to providing access to highly controlled systems.

FIRST ADVANTAGE AT A GLANCE:

- FBI channeler since the inception of the channeling program in 2006
- Channels directly to the FBI's Next Generation Identification (NGI) System
- Sole Channeler for the Financial Industry Regulatory Authority (FINRA)

KEY INSIGHTS:

Objective: Satisfy CJIS Security Policy IA requirements for channeler personnel with limited access to CJI.

Solution: HSPD-12 PIV-I credentials via NextgenID's PresenceID nationwide network, with a custom Match on Card fingerprint profile for offline biometric verification.

BUSINESS OUTCOMES:

- FBI CJIS Security Policy IA control family alignment
- Channeling compliance posture protected
- Eliminated travel costs and lost productivity
- Federally recognized solution deployed for a highly controlled environment
- Audit evidence reduced to a one-line reference

"You guys were the easy button, and I can't say enough good things about you."

- Channeling ISO, First Advantage Biometrics

Difficult path to build in-house: Though developing an internal CSP solution was considered, time to implementation and complexity of compliance would have been extremely costly due to the number of requirements in the IA control family. The opportunity cost for diverting resources that were working on other efforts would have been very high.

> ***"We have 74 pages of requirements we would either have to identify how we comply with line by line, or we can just demonstrate that we use an HSPD-12 credential. That was a no brainer."***
>
> - Channeling ISO, First Advantage Biometrics

SOLUTION:

One Credential. One Reference. Audit Closed.

The CJIS Security Policy contains a provision most non-Federal organizations would not know how to take advantage of: an HSPD-12 credential (including ones issued by a federally approved NFI, the gold standard for identity assurance) satisfies the entire IA section according to control IA-2. When a single credential can replace a complex IA control framework and operational overhead, the build-versus-buy conversation is brief.

NextgenID was the right provider for three reasons:

Federal authorization without federal bureaucracy: NextgenID holds federally approved NFI status. The credentials it issues carry the full legal weight of HSPD-12 compliance. When auditors ask about the IA section, First Advantage Biometrics' answer is a simple reference to NextgenID's published approvals.

A network delivered where the workforce operates: First Advantage Biometric personnel are mostly centralized in Portland, OR, but are also distributed nationwide. Whether near the secure facility or across the country, they can skip travel and complete credentialing locally at their nearest PresenceID location.

> ***"NextgenID provided a very easy avenue for compliance. The fact that they have a geographically dispersed network was really the driving factor."***
>
> - Channeling ISO, First Advantage Biometrics

Engineering depth for a non-standard problem: The biometric Match on Card requirement is not common, and most providers would not support it. NextgenID engineered a custom fingerprint profile enabling three-factor authentication (PIV card + PIN + fingerprint) completely offline and designed around the scanners First Advantage Biometrics already had on-site.

Michael Harris, CTO and EVP of NextgenID, was the principal architect and driving force behind the Match on Card innovation:

"No off-the-shelf solution existed for this environment. I brought that to leadership not as a problem but as a decision: do we build it or not. We built it. That required a genuine R&D commitment to technology that did not exist in the market. Watching a custom architecture go from whiteboard to a production system in a live FBI-connected environment, that is the kind of work I built this team to do."

– Michael Harris, CTO and EVP, NextgenID

DEPLOYMENT:

Prior Relationship. Fast Standup.

NextgenID, a trusted partner, brought immediate capability to address the CJIS Security Policy IA control family requirements. A kiosk was quickly deployed to the Portland facility and enrollment began shortly thereafter.

- **IT team enablement:** NextgenID functioned as a dedicated, ongoing technical partner throughout onboarding. Integration was collaborative; when questions came up, NextgenID had answers.
- **First remote IAL3 experience:** Previously limited to in-person credentialing, employees were guided through their enrollment by highly trained, certified remote agents for the first time. Feedback was clear: faster, simpler, and less disruptive than what came before.
- **Renewals built into operations:** Every three years, employees pre-register online and visit their nearest PresenceID kiosk once. Logistical and operational complexities are eliminated.

> ***"Even though we used to be a PIV-I provider, we don't have any folks in-house to do that anymore. Our IT resources had to relearn everything, they're still learning things, and NextgenID has been just a fantastic partner in helping us with that."***
>
> - Channeling ISO, First Advantage Biometrics

RESULTS:

The Audit Is Answered. The Business Need is Satisfied.

For an organization whose FBI Channeling is the foundation of its business, results are measured in risk removed:

FBI CJIS Security Policy IA compliance achieved. By referencing NextgenID's federally approved NFI status, First Advantage Biometrics provides auditors with a one-line compliance statement for the IA section. The answer to the multi-page IA control set fits in a single reference document.

Channeling compliance. First Advantage Biometrics' FBI compliance program is fully aligned with the most current version of the CJIS Security Policy. With a trusted partner's PIV-I solution, the core business line maintains a durable compliance posture.

Travel costs eliminated. Distributed personnel complete enrollment at their nearest PresenceID location. No flights, no hotels, no lost workdays.

Three-factor authentication in production. PIV card + PIN + fingerprint biometric: an entirely offline authentication system that is fully operational in a live channeling environment and built to a higher standard of authentication that most NFI PIV-I providers do not currently offer.

> ***"The solution was very streamlined, it was excellent. I mean just no complaints. I would absolutely recommend that any organization facing a similar compliance requirement should reach out to NextgenID."***
>
> - Channeling ISO, First Advantage Biometrics

WHAT THIS PROVES:

The Organizations That Need This Most Are the Ones Who Don't Know It Exists

All FBI channelers, state agencies with CJI access, and authorized recipients with statutory authority to use channelers face the same IA control family requirements and are still struggling with compliance. Most are working through it the hard way, documenting controls and building internal CSP programs, because they don't know that a single HSPD-12 credential from a federally approved NFI closes the audit conversation, and NextgenID is the critical enabler.

NextgenID is one of the few providers in the country that can deliver a solution with a nationwide network and the engineering capability to handle environments that don't fit a standard deployment profile. First Advantage Biometrics had the institutional knowledge to recognize the shortcut, and NextgenID had the infrastructure to deliver it.

Simplify Compliance. Start with NextgenID.

NextgenID delivers high-assurance identity proofing and enrollment through a nationwide network of secure identity stations and patented Supervised Remote Identity Proofing (SRIP) technology, now known as On-Site Unattended. NextgenID's platform enables organizations to verify identities anytime, anywhere, combining remote supervision, biometric capture, and NIST-compliant processes to streamline credentialing while maintaining the highest levels of security and compliance. Designed for federal, enterprise, and mission-critical environments, NextgenID reduces operational burden while accelerating secure onboarding at scale.

Take your first step towards CJIS compliance with NextgenID by contacting the team at:

(888) 373-8648

info@nextgenid.com

www.nextgenid.com

10300 Eaton Place, Suite 105
Fairfax, VA 22030, USA