CFSO
Consortium of Forensic Science Organizations

American Academy of Forensic Sciences
American Society of Crime Laboratory Directors
International Association for Identification
International Association of Coroners and Medical Examiners
National Association of Medical Examiners
Society of Forensic Toxicologists

INTEROPERABILITY ACROSS FORENSIC BIOMETRIC SYSTEMS

A National Strategy for AFIS/ABIS/MBIS Systems

Policy finding. The United States has mature exchange standards, but it lacks the coordinated governance, procurement requirements, testing, and sustained funding needed to make authorized cross-jurisdictional forensic information exchange routine.

The Problem

The most significant and arguably most urgent concern pertains to the Automated Biometric Identification Systems (ABIS). Also known as the Automated Fingerprint Identification System (AFIS) and currently referred to as Multimodal Biometric Identification Systems (MBIS), these systems have been in operation since the mid-1980s. They facilitate electronic searches of fingerprint and other biometric records to identify potential terrorists and criminal suspects, report criminal histories, assist in forensic investigations, and conduct civil background checks.

Despite their longstanding and critical role, ABIS/AFIS/MBIS platforms—and the laboratory, medical examiner and coroner, death-registration, missing-person, and investigative systems that support them—frequently use different formats, identifiers, access rules, and interfaces. Vertical biometric searching from local and state repositories to the FBI's Next Generation Identification system is well established, but horizontal peer-to-peer searching among neighboring jurisdictions remains limited. Consequences include missed investigative opportunities, duplicate entry, re-encoding of latent-print features, delayed coordination, data-quality errors, vendor lock-in, and unequal capability among smaller and tribal agencies.

Standards Exist—Implementation Lags

ANSI/NIST-ITL 1-2025 (NIST SP 500-294), approved in January 2026, provides the current vendor-neutral framework for exchanging biometric and biographic information. For latent prints, NIST SP 1152—the Latent Interoperability Transmission Specification—supports both hierarchical and peer-to-peer exchange, while NIST SP 1155 and SP 1156 provide procurement and interagency-agreement guidance. These standards are necessary, but format compliance alone does not ensure that systems interpret data consistently or perform reliably across vendors. Operational interoperability also requires shared definitions, legal authority, trusted security controls, validated workflows, service agreements, training, and end-to-end conformance testing.

Recommended National Action

- Establish accountable federal governance. DOJ, working with NIST, FBI, NIJ, BJA, DHS, state, local, county, tribal, professional, privacy, and vendor stakeholders, should maintain implementation profiles, performance measures, legal and privacy guidance, and a public roadmap.
- Tie federal funding to testable requirements. Grants supporting AFIS/ABIS/MBIS acquisition or major upgrades should require current standards, documented interfaces, data export, migration support, audit logging, and independent acceptance testing, with phased assistance for resource-limited jurisdictions.

- Modernize procurement. Model solicitations and agreements should address transaction behavior, response content, performance, cybersecurity, data ownership, version upgrades, vendor cooperation, and contract exit rights—not merely file format.
- Develop a federated biometric exchange capability. A federal feasibility study should compare centralized, federated, and hybrid approaches. A federated service could provide routing, authorization, validation, discovery, and auditing while jurisdictions retain repository control and permitted-use rules.
- Fund lifecycle readiness and extend the framework. Support legacy-data migration, provenance preservation, conformance and security testing, training, and continuing operations; then develop discipline-specific profiles for LIMS, medicolegal death investigation, EDRS, NamUs, and other priority systems.
- Build privacy, civil-rights, and security protections into every exchange. Apply purpose limitation, least privilege, strong authentication, encryption, immutable auditing, retention rules, incident response, quality monitoring, access review, and redress where applicable.

Implementation and Accountability

Implementation should proceed in stages: establish governance and baseline metrics; publish profiles and test suites; pilot cross-vendor, cross-jurisdictional exchanges; scale through grants and shared services; and sustain the capability through recurring certification and version management. Progress should be measured by repository coverage, successful authorized queries, response time, conformance results, data quality, audit findings, investigative value, and equitable participation.

Conclusion

Interoperability is national forensic infrastructure, not an optional vendor feature. A durable solution may not require replacing every platform with one database. It requires enforceable common requirements, trusted exchange services, independent testing, modern procurement, privacy and security safeguards, and shared governance. The FBI NGI system should be expanded and explored as an essential tool, however, coordinated federal leadership can convert existing standards into a reliable national capability while preserving local control and lawful limits on access.

Selected References

CFSO. (2023). Automated Biometric Identification System (ABIS) Interoperability.

International Association for Identification. (2022). Report on ABIS Interoperability.

NIST. (2026). ANSI/NIST-ITL 1-2025: Data Format for the Interchange of Biometric and Biographic Information (SP 500-294). https://doi.org/10.6028/NIST.SP.500-294

Taylor, M. K., et al. (2013). Latent Interoperability Transmission Specification (NIST SP 1152). https://doi.org/10.6028/NIST.SP.1152

Ropero-Miller, J. D., et al. (2022). Data Exchange Practices of Medicolegal Death Investigation. Forensic Technology Center of Excellence.

POC: Beth Lavach, bethlavach@elsandassociates.com, 703-622-8752