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

Federal Support Needs for Emerging Technologies in Forensic Science

Accelerating responsible innovation, validation, adoption, and operational readiness across forensic science

Executive Summary:

The forensic science community is entering a period of rapid technological advances driven by artificial intelligence, complex analytics, digital evidence, automation, next-generation sequencing, novel sensing platforms, and increasingly innovative data environments. These capabilities can improve speed, accuracy, consistency, and investigative value, but only if they are validated, governed, funded, and implemented in ways that preserve scientific integrity and public trust.

The federal government plays a critical role in helping laboratories, medical examiner and coroner offices, law enforcement agencies, courts, researchers, and standards bodies bridge the gap between promising technology and reliable practice. Federal action is required to strengthen research and development, establish standards and test methods, fund implementation, expand training, support workforce modernization, and create mechanisms for coordinated technology transition.

Background:

Forensic science supports public safety, criminal investigations, prosecutions, defense review, exonerations, disaster response, missing-person investigations, and national security. Yet many forensic service providers face persistent backlogs, aging infrastructure, fragmented data systems, workforce shortages, and uneven access to modern analytical tools. Emerging technologies offer meaningful relief, but they also introduce new risks related to validation, bias, explainability, quality assurance, cybersecurity, privacy, admissibility, and procurement.

Federal initiatives currently provide important foundations. The National Institute of Justice supports forensic research, technology transition, and practitioner engagement through mechanisms such as the Forensic Technology Center of Excellence and forensic technology working groups. The National Institute of Standards and Technology advances measurement science, standards, digital forensics resources, and foundational studies. The Department of Justice also maintains federal forensic capabilities and supports coordination across federal, state, local, and tribal partners. However, the pace and breadth of emerging technologies require a more integrated national approach.

Priority Needs from the Federal Government:

1. <u>Sustained Research, Development, Testing, and Evaluation</u>: Federal investment in applied research that addresses operational problems is needed. Priority areas include AI-assisted pattern recognition, probabilistic interpretation, digital and multimedia evidence, rapid toxicology, advanced DNA methods, forensic genetic genealogy governance, automated evidence triage, robotics, portable instrumentation, and resilient laboratory information systems. Federal RDT&E should emphasize independent testing, benchmark datasets, uncertainty quantification, reproducibility, known limitations, and performance across realistic case conditions. Programs require practitioner input from project design through field evaluation so that outcomes are usable in accredited laboratories and defensible in court.

2. <u>Standards, Validation Pathways, and Conformity Assessment</u>: Forensic providers need clear federal support for standards and validation pathways that help determine when emerging technologies are ready for operational use. This includes common test methods, reference materials, data quality requirements, model documentation, performance thresholds, auditability expectations, and guidance for implementation in accredited environments. For AI-enabled tools, the community needs standards for training data provenance, bias assessment, explainability, human oversight, error-rate reporting, cybersecurity, model change management, and post-deployment monitoring. Federal standards leadership is essential to ensure technologies improve reliability rather than introduce opaque or inconsistent practices.

3. Funding for Adoption, Infrastructure, and Sustainment: Many agencies cannot adopt validated technologies because they lack capital funding, IT modernization resources, cybersecurity capacity, staffing, and sustainment budgets. Federal grants should support the full implementation lifecycle: procurement, integration, validation, accreditation requirements, training, maintenance, data migration, security controls, and lifecycle replacement. Funding models should account for smaller, rural, tribal, and resource-constrained providers that may not have dedicated grant-writing or technology-transition staff. Shared service models, regional centers, cloud-enabled platforms, and cooperative purchasing could reduce inequities in access to modern forensic capabilities.

4. Workforce Development and Change Management: Emerging technologies change the skills required of forensic professionals. The federal government should support training in data science, AI literacy, statistics, digital evidence, cybersecurity, validation science, quality assurance, courtroom communication, and ethical technology use. Training should be modular, discipline-specific, and available to scientists, managers, investigators, prosecutors, defenders, judges, and policymakers. Federal support should also address workforce recruitment and retention through fellowships, cross-training, internships, academic partnerships, continuing education, and career pathways that combine forensic science with computing, engineering, statistics, and information assurance.

5. Data Governance, Interoperability, and Cybersecurity: Forensic data is growing in volume, variety, and sensitivity. Digital evidence, body-worn camera footage, cloud data, DNA profiles, toxicology results, laboratory notes, images, and machine-generated outputs require secure, interoperable, and well-governed data environments. Federal leadership is needed to define common data models, metadata requirements, chain-of-custody practices, access controls, retention guidance, and secure information-sharing approaches. Cybersecurity should be treated as a core element of forensic reliability. Laboratories need support for secure cloud adoption, identity management, vulnerability management, incident response, vendor risk management, and continuity planning so that evidence systems remain trustworthy and available.

6. Ethical, Legal, and Policy Frameworks: Emerging forensic technologies can raise legal and ethical questions involving privacy, civil liberties, algorithmic bias, disclosure, admissibility, explainability, and equitable access. Federal agencies should convene practitioners, researchers, defense and prosecution stakeholders, judges, community representatives, privacy experts, and standards bodies to develop practical governance frameworks. Guidance should clarify expectations for documentation, statements of limitations, discovery, validation records, human review, error communication, and responsible use. The goal should be to promote innovation while ensuring that technology strengthens due process, transparency, and public confidence.

Recommended Federal Actions:

1. Create a national roadmap for emerging forensic technologies that aligns research, standards, funding, training, and implementation priorities.
2. Expand practitioner-led technology working groups to continuously identify operational needs and evaluate barriers to adoption.
3. Fund independent validation centers and reference datasets for AI, digital evidence, probabilistic interpretation, and advanced laboratory methods.
4. Establish grant programs that cover full-lifecycle adoption costs, including sustainment and cybersecurity.
5. Support standards development and conformity assessment for emerging forensic tools, including AI-enabled systems.
6. Develop national training curricula and credentialed learning pathways for emerging forensic technologies.
7. Promote interoperable, secure, and privacy-preserving data systems across forensic disciplines and jurisdictions.
8. Convene legal and ethical policy forums to address admissibility, disclosure, civil liberties, and responsible use.

Point of Contact: Beth Lavach bethlavach@elsandassociates.com | (703) 622-8752