Biometrics Institute Concepts and Solutions Report

Biometrics: Keeping it Real

March 2026 **Silver Jubilee edition** celebrating 25 years of Responsible Biometrics

SAIC: A 'Real' Look at Evaluating Biometric and Identity Systems for Remote Identity

The biometrics and identity landscape is rapidly evolving as advances in artificial intelligence make it possible to perform biometric recognition at scale, including to reduce fraud in online transactions. Remote identity systems expand access and convenience, but they also introduce new risks. Even as biometric technologies reach higher performance benchmarks, threats such as deepfakes, digital injection attacks and uneven performance across devices and demographic groups can undermine public trust and real-world effectiveness of biometric systems.

To preserve the security and fraud fighting potential of remote identity systems, they must operate consistently and reliably across diverse environments and user populations. Independent verification of vendor performance claims is essential to maintaining public confidence, confirming security can be maintained while ensuring low user rejection rates.

Why Rigorous Biometric Evaluation Matters

Operational performance in biometric and identity systems, including remote identity systems, must be measured accurately, quickly and consistently to keep pace with technological change. Independent research from government, industry and academic sources highlights persistent performance gaps that can reduce usability and erode trust.

Key findings include:

- **Demographic variation:** A recent General Services Administration study found that the median true accept rate for genuine users was only 85% across five tested systems, with significant differences in performance across demographic groups.[1]
- **High user rejection rates:** The Department of Homeland Security Science and Technology Directorate evaluated 3,024 combinations of presentation attack detection, face recognition and document validation technologies. The median system accepted only 46% of genuine users, and fewer than 1% of combinations met both security and user facilitation targets.[2]
- **Device and environment sensitivity:** Research shows that user devices, document types and testing conditions affect system performance, with direct implications for reliability and public confidence.[3]

Taken together, these findings show that capable technologies do exist. However, success depends on strategic ongoing evaluation and selection of system components. Deployment of a system to meet compliance requirements, absent independent evaluation, does not provide assurance of acceptable performance. Performance verification before deployment and throughout operations is required to ensure systems perform as expected and continue to meet real-world demands.

Barriers to Effective Biometric Testing

Despite its importance, comprehensive testing of biometric and identity systems remains challenging for many organisations due to several barriers, including:

- **Data privacy and access:** Limited availability of sequestered data that reflects real-world conditions makes reliable and repeatable testing hard to achieve.
- **Cost and complexity:** Testing at scale is expensive and requires specialised expertise. Fragmented system architectures further complicate evaluation, particularly when security and user facilitation must be assessed independently.

---

[1] Center for Identification Technology Research. (2024) *"A Large-Scale Study of Performance and Equity of Commercial Remote Identity Verification Technologies Across Demographics."* arXiv preprint, https://arxiv.org/pdf/2409.12318

[2] DHS Science and Technology Directorate. (2025) *"A Quantitative Framework for Evaluating Remote Identity Validation Systems: Technical Demonstration Analysis and Evaluation."* DHS S&T Technical paper series, https://www.dhs.gov/science-and-technology/publication/quantitative-framework-evaluating-remote-identity-validation-systems

[3] SAIC Identity and Data Sciences Laboratory. (2026) "*Robustness of Presentation Attack Detection in Remote Identity Validation Scenarios.* arXiv preprint, https://arxiv.org/abs/2602.00109

- **Reliance on vendor-led testing:** Performance claims provided by vendors may not reflect operational use or are often difficult to compare across solutions.
- **Resource constraints:** Many organisations lack the funding and capacity to build and maintain in-house testing capabilities.

These barriers limit informed decision-making and increase the risk of deploying systems that fall short in operational environments.

A Path Forward: Testing as a Service

Collaborative, independent testing as a service (TaaS) solutions provide a practical way to address challenges and build confidence in biometric and identity systems. Effective test service providers deliver scalable, objective testing that supports operational readiness and informed decision-making. With the right test infrastructure in place, teams can conduct rapid, repeatable evaluations at scale, producing performance metrics trusted by both government and industry organisations.

1. **Continuous testing without disruption:** TaaS enables repeatable testing processes using sequestered data collected in simulated operational environments, without interfering with day-to-day activities. Clients can establish a testing cadence aligned to their needs, while the competent test service provider brings the testing infrastructure, expertise and innovation to bear for the client.
2. **Component-level insights:** By evaluating individual subsystems such as presentation attack detection and face recognition, TaaS provides clearer visibility into what is performing well and where limitations exist, helping decision-makers identify weaknesses, isolate bottlenecks and target improvements.
3. **Standards-based evaluation:** Established biometric standards provide a common framework for understanding performance metrics, allowing clients to assess and compare technologies on equal footing.
4. **Sequestered data testing:** Unlike vendor testing that may rely on reused training data, independent TaaS evaluation uses protected, operationally relevant datasets that better predict real-world performance.
5. **Streamlined procurement:** Regular assessment of commercial solutions outside of a specific acquisition cycle provides early insight into performance trends, helping shorten procurement timelines and adapt technology selection to dynamic threats and innovation.

Test Early. Test Often.

Ongoing testing helps ensure biometric and identity systems continue to meet requirements as technology evolves and attackers introduce new techniques. Changes made after deployment can unintentionally degrade performance if issues are not identified early. A testing as a service framework supports continuous, scalable evaluation to reduce risk and protect mission-critical operations.

Conclusion

Biometric systems for remote identity offer significant promise, but they also face real challenges in delivering accurate, secure and reliable performance. Meeting operational demands and sustaining public trust requires ongoing evaluation. Testing as a service supports informed technology selection and monitoring while reducing risks tied to demographic disparities, environmental variations and emerging threats. Through an agile, standards-driven testing approach, clients are empowered to make data-driven decisions that strengthen identity solutions and user confidence.

Organisation: Science Applications International Corporation (SAIC)
Name: Yevgeniy Sirotin, Technical Director, SAIC Identity and Data Sciences Laboratory (IDSL)
Telephone number: +1 781 710 3472
Contact details: yevgeniy.b.sirotin@saic.com
Name: Jerry Tipton, Executive Director, Integrated Security Technologies and Programs
Telephone number: +1 301 909 9263
Contact details: jerry.l.tipton@saic.com

RESPONSIBLE BIOMETRICS

2001 BIOMETRICS™ INSTITUTE 2026

SILVER JUBILEE

A global community promoting the **responsible**, **ethical** and **effective** use of biometrics since 2001

biometricsinstitute.org