

U.S. Department of Homeland Security

SCIENCE AND TECHNOLOGY DIRECTORATE

Remote Identity Validation Activities



Science and
Technology

Yevgeniy Sirotn
The Maryland Test Facility

Arun Vemury
Senior Advisor, Biometrics and Identity
DHS S&T

September 30, 2026

Agenda

- Background
- Remote Identity Validation Rally 2 (RIVR-2) Announcement
- RIVR-X Biometric Deepfake Detection
- Biometric and Identity Deepfake Expert Technical Exchange
- Schedule and Next Steps



[SCIENCE AND TECHNOLOGY DIRECTORATE]

Operationalizing science and technology.

The Science and Technology Directorate (S&T) researches, develops, tests, and evaluates solutions needed to meet the growing demands of our nation's homeland security officials.

- We capture specific mission needs.
- We deliver impactful technology solutions.
- We conduct independent test and evaluation.





Biometric & Identity Technology Center

S&T conducts foundational research to ensure advancements in science and technology are harnessed for cutting-edge solutions to new and emerging operational challenges.

- ✓ Drive biometric and identity innovation at DHS through research development, test and evaluation (RDT&E) capabilities
- ✓ Facilitate and accelerate understanding of biometrics and identity technologies for new DHS use cases
- ✓ Drive efficiencies by supporting cross cutting methods, best practices, and solutions across programs
- ✓ Deliver subject matter expertise across the DHS enterprise
- ✓ Engage industry and provide feedback
- ✓ Encourage innovation with industry and academia



Remote Identity Validation (RIV)

- RIV systems verify the identity of users based on data, including face images and document images, submitted over the internet using personal electronic devices, such as smartphones.
- Remote Identity Validation (RIV) systems integrate multiple algorithmic subsystems to validate the identity evidence presented by users.
 - Reduce friction for genuine users; and
 - Guard against identity fraud.
- DHS S&T sponsors evaluations of each RIV subsystem to:
 - Make it easier for organizations to understand the current effectiveness of these systems; and
 - Identify performance gaps.

Remote Identity Validation Rally (RIVR)

- Prior evaluations of RIV technologies:
 - Sponsored by DHS S&T.
 - Remote Identity Validation Technology Demonstration (RIVTD) from 2023 to 2025.
 - 2025 Remote Identity Validation Rally (RIVR-1) from 2025 to 2026.
- Performance gaps:
 - Excessive friction for legitimate users; and
 - Excessive vulnerability to some fraud vectors.



FIRST REMOTE IDENTITY VALIDATION RALLY (RIVR-1): CONVENIENCE

Remote Identity Validation User Workflow



Document Validation
7 Systems

79%
Success Rate
(Median)



Presentation
Attack Detection
18 Systems

96%
Success Rate
(Median)



Selfie Match
To Document
16 Systems

99%
Success Rate
(Median)

Full Workflow

75%

Composite* Success Rate



REJECTED

ACCEPTED

ACCEPTED

REJECTED

REJECTED

ACCEPTED

VALIDATED

FIRST REMOTE IDENTITY VALIDATION RALLY (RIVR-1): SECURITY

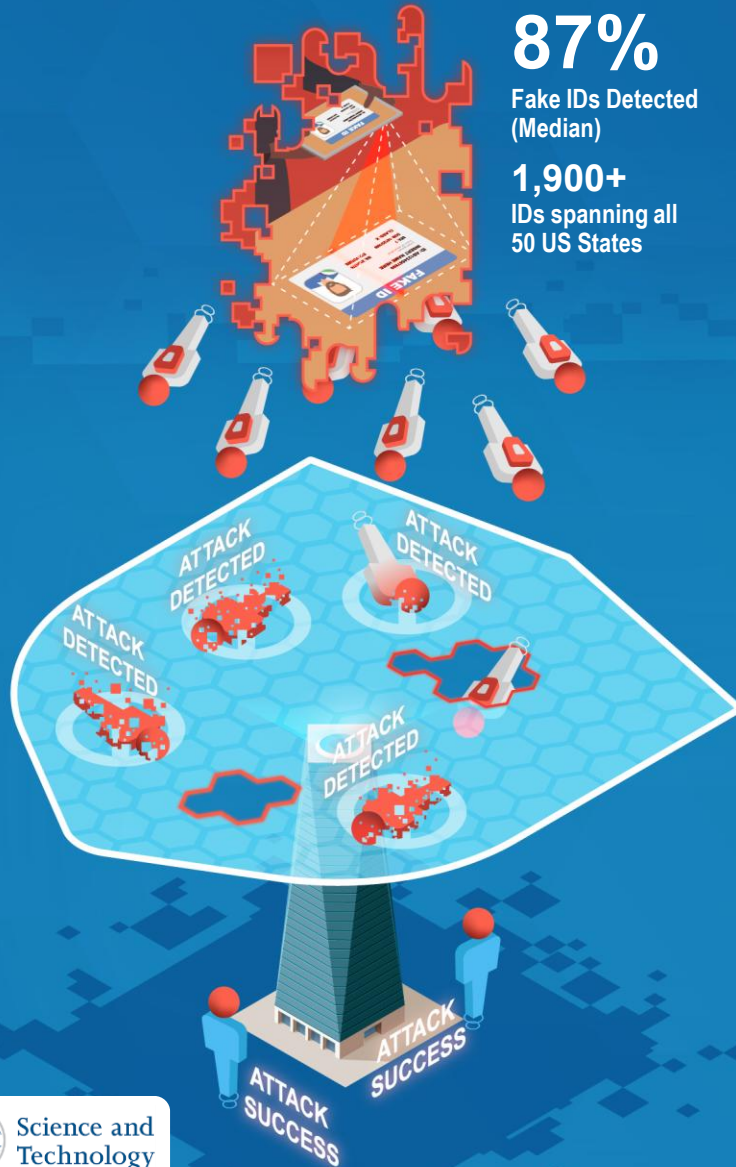
Document Validation

87%

Fake IDs Detected
(Median)

1,900+

IDs spanning all
50 US States



Presentation Attack Detection

53%

Presentation Attacks
Detected (Median)
*based on most successful attack

1,500+

Attack Presentations



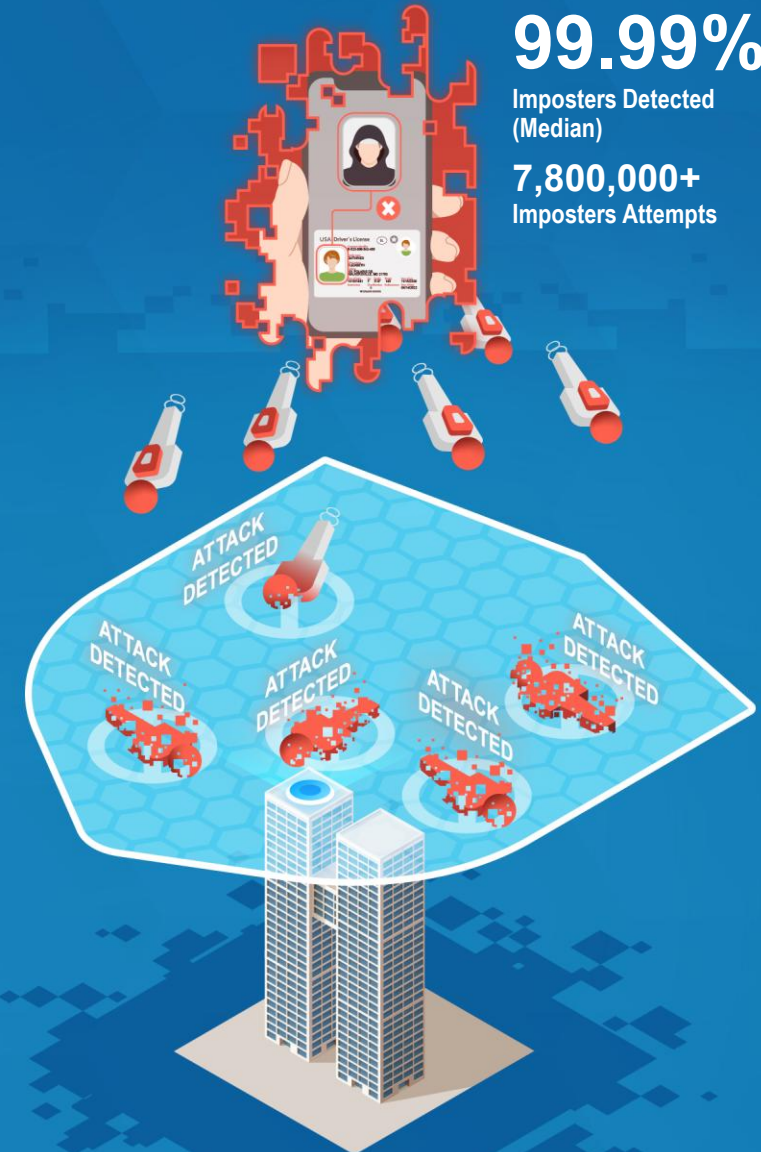
Selfie Match To Document

99.99%

Imposters Detected
(Median)

7,800,000+

Imposters Attempts



Science and
Technology

Ongoing RIVR Evaluations

- The results of prior testing and the emerging threats posed to RIV systems from fraud based on generative artificial intelligence (AI) support the need to perform ongoing evaluations.
- DHS S&T plans to continue and expand RIVR evaluations:
 - Plan for a faster biannual evaluation cadence in the future
 - Main **RIVR** Tracks:
 - Selfie Match to Document (SMTD)
 - Identity Document Validation (IDV)
 - Presentation Attack Detection (PAD)
 - Experimental **RIVR-X** Tracks:
 - Biometric Deepfake Detection (BDD)

Ongoing RIVR Evaluations

- **Technology Gaps and Innovation:**
 - DHS S&T will identify key areas where RIV vendors should focus improvements.
 - Companies can refine their technologies and participate in re-evaluation.
- **RIVR-2 and RIVR-X:**
 - Allow companies to take risks on new challenges.
 - Results are aliased by default.
 - Companies can self-attest participation.
- **RIVR-3+ (future):**
 - Results associated with company names by default.
 - Companies demonstrate system maturity by participating.
 - Email peoplescreening@hq.dhs.gov for questions.



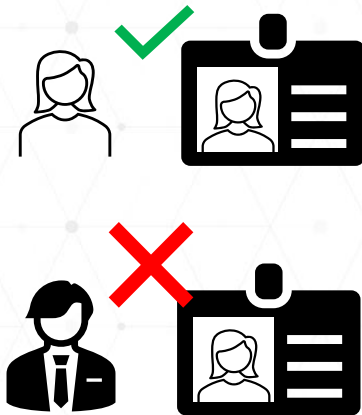
Second Remote Identity Validation Rally (RIVR-2)



RIVR-2 Evaluation Tracks

Selfie Match to Document (SMTD)

- 1:1 Verification



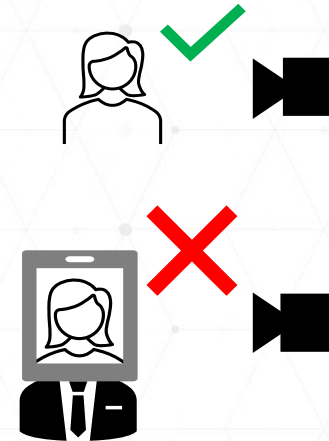
ID Validation (IDV)

- Reject fraudulent documents



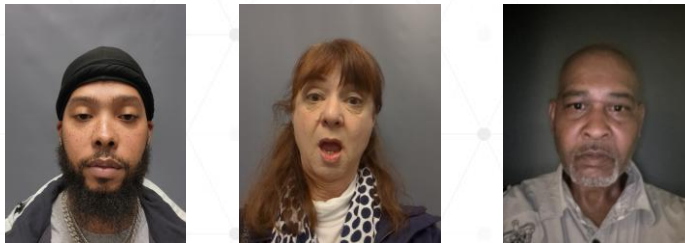
Presentation Attack Detection (PAD)

- Reject screens and printouts
- Reject masks and other presentation attacks



RIVR-2 Selfie Match to Document

- RIVR evaluates the ability of SMTD systems to determine if a smartphone **selfie image** is the same person as pictured on a **U.S. State-issued ID cards**.
- Biometric comparisons include:
 - Selfie photo images.
 - Photo on genuine U.S. State-issued ID cards (e.g., driver's licenses).
 - **NEW!** Common selfie quality degradations including photos taken in low light.
- Sample Images:



All volunteers shown here consented to have their images used in government presentations.



Note – Sampling of driver's license not shown for privacy reasons. Sample driver's licenses taken from:

[What do the new Maryland driver's licenses look like? \(wbaltv.com\)](http://wbaltv.com)



RIVR ID Validation

- RIVR evaluates the ability of IDV systems to establish the authenticity of US state and territory-issued ID cards and international passports based on images gathered using smartphones.
- IDs include:
 - Driver's licenses and non-license state ID cards issued by US states or territories (front and back images).
 - **NEW!** International passports (face page images).
- Evidence validation processes:
 - Test identity evidence for authenticity against document type libraries for **information completeness**, **format**, and **correctness**;
 - Test identity evidence for authenticity through **tamper and counterfeit detection** (including deepfake); and
 - Test identity evidence for authenticity by **validating and confirming presence of security features** for the type of evidence presented.

DHS S&T's RIVTD helped inform NIST SP 800-63A evidence validation standards

- Defined performance measures
- Informed acceptable performance levels

[NIST SP 800-63A-4 second public draft, Digital Identity Guidelines: Identity Proofing and Enrollment](#)

3.1.12. Requirements for Evidence Validation Processes (Authenticity Checks)

Evidence validation can be conducted by remote optical capture and inspection (often called document authentication or doc auth) or conducted by visual inspection of a trained proofing agent or trusted referee. CSPs may employ either or both processes for evaluating the authenticity of identity evidence.

The following requirements apply to CSPs that employ optical capture and inspection for the purposes of determining document authenticity:

1. Automated evidence validation technology **SHALL** meet the following performance measures:
 - Document false acceptance rate (DFAR) of .10 or less. ⁶
 - Document false rejection rate (DFRR) of .10 or less. ⁷

RIVR-2 Presentation Attack Detection

- RIVR evaluates PAD systems on their ability to differentiate between selfies of bona-fide users and presentation attacks.
- Presentation attacks are performed through use of various attack instruments.
(updated regularly)
- Two PAD system types are in scope:
 - Passive PAD;
 - Active PAD.

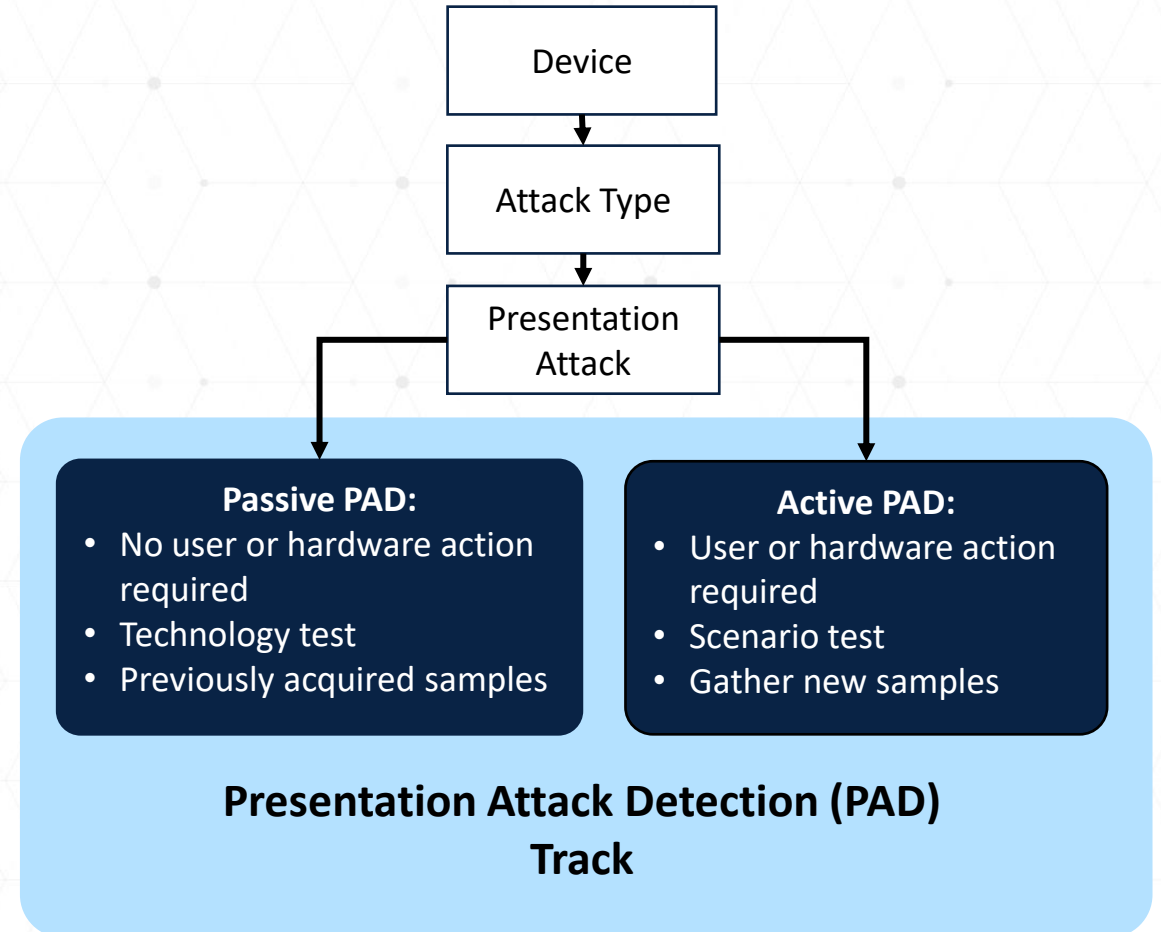


Active PAD user action:

- Turn / rotate head, blink, etc.

Active PAD hardware action:

- On-board cameras, sensors, etc.



RIVR-X Biometric Deepfake Detection



RIVR-X Biometric Deepfake Detection (BDD)

- Biometric deepfakes are images where the identity characteristics are generated or manipulated using AI tools.
- Both deepfake selfie images and deepfake document images can be used to attack RIV systems.
- RIVR-X BDD track will demonstrate the ability of commercial deepfake detectors to differentiate between deepfake attacks and bona-fide samples.
- Technologies submitted to RIVR IDV can opt-in to participating in detection of document images with manipulated face photos or document fields.
- BDD is planned for early 2027.

NEW!

Biometric Deepfake Detection (BDD)

- Reject biometric deepfake images and videos
- Reject manipulated or synthetic images of documents
- Share challenging deepfakes



[TikTok Tom Cruise deepfake creator: public shouldn't worry about 'one-click fakes' | The Verge](#)

RIVR-X Biometric Deepfake Detection (BDD)

- Deepfakes can come from a variety of generation methods.
- RIVR-X BDD will accept submissions of detectors, deepfake datasets, and methods of deepfake data generation.
- Datasets will be submitted by a variety of organizations.
- Vendors submitting detectors will have to provide a sample deepfake image dataset:
 - 1,000 images.
 - Detected well by your system.
 - Difficult for other systems to detect.
- Comparing detectors against generation methods will:
 - Identify difficult to detect deepfake generation methods.
 - Assess whether detectors generalize across deepfake generation methods.

NEW!

Biometric Deepfake Detection (BDD)

- Reject biometric deepfake images and videos
- Reject manipulated or synthetic images of documents
- Share challenging deepfakes



[TikTok Tom Cruise deepfake creator: public shouldn't worry about 'one-click fakes' | The Verge](#)

Biometric and Identity Deepfake Detection Technical Exchange

- DHS S&T plans to host technical exchange meetings with government and industry experts.
- **Goals:**
 - Develop of a framework for ongoing evaluations for biometric deepfake detectors using various sources of genuine and biometric deepfake media.
 - Increase awareness of commercial technology performance while respecting and protecting intellectual property.
- Government and industry experts discuss methods of collecting and updating relevant test data in a manner to ensure evaluation results provide information suitable to:
 - Promote awareness of emerging threats;
 - Improve overall industry biometric deepfake performance.
- Email peoplescreening@hq.dhs.gov if interested in participating.

RIVR-2 Timeline



Dates subject to change, check <https://mdtf.org/Rivr2> for current schedule.

RIVR-2 Next Steps

- Key Upcoming Dates:
 - **October 16**, 2026 – Applications for IDV and SMTD due
 - **October 30**, 2026 – Notification of acceptance
 - **November 20**, 2026 – IDV and SMTD systems provided for testing
- Participation Requirements:
 - Participation will require executing a Cooperative Research and Development Agreement (CRADA) with DHS S&T
 - All systems must conform to MdTF APIs and technical requirements specific to each track
- Additional track-specific information will be provided at <https://mdtf.org/Rivr2>:
 - Technical Requirements
 - Evaluation Metrics
 - Application to Participate

- Email peoplescreening@hq.dhs.gov for:
 - Questions about the CRADA process
 - To be notified about RIVR-2 results
 - Announcements regarding the upcoming tracks

- Email rivr@mdtf.org for:
 - Questions about technical requirements
 - Questions about evaluation metrics