# 2023 Remote Identity Validation Technology Demonstration – Track 3 - Presentation Attack Detection – Application Instructions

Identity Validation technology providers may apply to participate in the Remote Identity Validation Technology Demonstration (RIVTD). Additional information about the RIVTD is available at https://mdtf.org/rivtd, including but not limited to, slides from informational webinars.

These application instructions are specifically for the **RIVTD Track 3 - Presentation Attack Detection (PAD)**. This track is intended as an initial step to survey the current state of presentation attack detection systems and technologies. The application process provides an opportunity for interested parties to describe their respective companies and the capabilities and performance of your presentation attack detection technology.

**All application materials are due by February 29, 2024 at 11:59PM Eastern Standard Time. All application materials should be sent to peoplescreening@hq.dhs.gov and rivtd@mdtf.org.**

Applications SHALL include a white paper in pdf format, up to five (5) pages in length.
Any proprietary materials included in the application SHOULD be clearly marked.
Whitepapers SHALL include the following information:

1. **Description of the company:**
    - Company name, location (including country of headquarters), and year formed.
    - Contact information (name, email, telephone number) of a:
        - Business representative.
        - Technology representative.
    - Provide a brief description of company history, experience in the identity validation community, and the primary markets served.
    - Describe any remote identity validation technologies offered: Document Validation, Face Matching, Face Liveness / Presentation Attack Detection, Other.
2. **Presentation attack detection system overview:**
    - When was the PAD system first conceived and developed? Is it still under development?
    - Where was the PAD source code developed and what security controls are implemented?
    - Does the PAD system have any current active deployments? If so, describe them.
    - Describe the complexity and maturity of your PAD system, including a high-level overview of the underlying PAD technology.
    - Describe the types of presentation attacks the system can detect. Are there known presentation attack detection issues?
    - Is your PAD system active (i.e., requires on-device sensors and/or interaction with the user) or passive (i.e., a software only solution that can detect attacks from pre-recorded images and/or videos)?

Continued on the next page.

3. **Presentation attack detection system technical description:**
    - Can your PAD system operate without any access to the internet, and with no access to cloud infrastructure?
    - *ACTIVE PAD SYSTEMS ONLY:*
        - Describe how you be able to demonstrate your PAD system on an iOS and an Android smartphone. Are all required computations performed on the smartphone device? If not, please describe how you will install your PAD system and implement any required back-end functionality at the Maryland Test Facility (MdTF) for the test.
        - Provide a list of all required hardware and sensor components.
        - Describe the actions that a user must take to use your PAD system (e.g., blinking or head turning).
        - How long does it take for the PAD system to perform a single user transaction?
        - Describe how you will handle break / fix issues encountered during testing?
    - *PASSIVE PAD SYSTEMS ONLY:*
        - Describe how you will provide your PAD system within a single Docker container for demonstration.
        - Provide an estimate of the following properties of the docker container with your PAD system:
            - Recommended CPU,
            - RAM,
            - Disk space, and
            - Operating system.
        - List any additional dependencies.
4. **Presentation attack detection system inputs and data processing steps:**
    - *ACTIVE PAD SYSTEMS ONLY:*
        - How will users initiate a transaction with your PAD system?
        - Describe how your system will interact with and instruct users during a PAD transaction.
        - Describe how your PAD system will evaluate the user transaction and provide results through the MdTF Active PAD system API?
    - *PASSIVE PAD SYSTEMS ONLY:*
        - Does your system operate on still "selfie" images? If yes, list any image requirements and supported file formats.
        - Does your system operate on video? If yes, list any requirements including user behavior (e.g., blinking or head turning), the duration of the video, and supported file formats.
        - Describe how your system evaluate the images or videos provided through the MdTF Passive PAD system API?

Continued on the next page.

5. **Presentation attack detection system outputs:**
    - How will the required MdTF API *PADOutcome* be determined?
    - How will the required MdTF API *PADScore* be determined?
    - Will *PADProperties* be provided? What properties are returned?
    - *ACTIVE PAD SYSTEMS ONLY:*
        - Please describe the *BiometricSample* to be returned for each transaction.
    - What other outputs should be considered for demonstrating your PAD system?
6. **Presentation attack detection system performance estimates:**
    - Describe any measurements of performance of the presentation attack detection system and how they were tested, including references to any whitepapers, performance benchmarks, and/or benchmark datasets used.
    - Provide estimates of performance for the following metrics:
        - Expected System Error Rate,
        - Expected Attack Presentation Classification Error Rate (APCER) @ Bona fide Presentation Classification Error Rates (BPCER = 1:10, 1:100, 1:1000, 1:10000),
        - Expected time to complete a transaction.
    - Provide estimates of system stability to age, gender, race, and skin tone.