# 2023 Remote Identity Validation Technology Demonstration

## Match to ID Application Instructions

Identity Validation technology providers may apply to participate in TRACK 2 (Match to ID) of the 2023 Remote Identity Validation Technology Demonstration (RIVTD). Additional information about the 2023 RIVTD is available at https://mdtf.org/rivtd, including but not limited to slides from informational webinars.

**These application instructions are specifically for the Match to ID track. The Match to ID track portion of the demonstration is intended as an initial step to survey the current state of remote identity technology. It is an opportunity for you to describe and demonstrate the capabilities and performance of your Match to ID technology.**

**All application materials are due by June 22, 2023 at 11:59PM Eastern Standard Time. All application materials should be sent to peoplescreening@hq.dhs.gov and rivtd@mdtf.org.**

Applications MUST 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 MUST include the following information:

1. **Company overview:**
    - Company name, location (including country of headquarters), and year formed.
    - Contact information (name, email, telephone number) of a business representative and, separately, a 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. **Match to ID system overview:**
    - Describe the complexity and maturity of your match to ID system, including a high-level overview of the underlying match to ID technology.
    - When was the system first conceived and developed? Is it still under development?
    - Where was the source code developed and what security controls are implemented?
    - Are there examples where the product is in use now?
3. **Match to ID system technical capabilities:**
    - State the recommended CPU, RAM, disk, and operating system. List any runtime dependencies.
    - Can the system be provided as a single Docker image under 1.5GB in size?
    - What are the acceptable document types: Passports, US Drivers Licenses, Other?
    - Are there known issues that limit performance (image size, pixels between the eyes, face pose, document wear, etc.)?
4. **Match to ID system inputs and data processing steps:**
    - What are the required system inputs (supported image formats, etc.)?
    - What image restrictions / limitations / requirements does your system have?
    - How will your system process the selfie and document images provided through the MdTF API?

- Describe how your system generates a biometric face template from a selfie, and from an ID document image.
- Describe how your system generates a 1:1 match score between two face templates.

5. **Match to ID system outputs:**
    - Describe how your system will generate a face template from a selfie and from an ID document image and return it in accordance with the MdTF API.
    - Describe how your system will generate 1:1 similarity scores between templates and return them in accordance with the MdTF API.
    - How were the biometric matching thresholds for your system established?
    - What other outputs should be considered for your system?
6. **Match to ID system performance estimates:**
    - Has the underlying biometric algorithm been evaluated in NIST FRVT? If so, under what system name and what was the performance?
    - Describe any additional measurements of the performance characteristics of the match to ID system and how it was tested, including references to any whitepapers, performance benchmarks, and/or benchmark datasets used.
    - Provide estimates of performance for the following metrics:
        - Expected failure to process rate (unable to create a template)
        - Expected true match rate and matching thresholds for the following false match rates:
            - @ 1:10,000 FMR
            - @ 1:100,000 FMR
            - @1:1,000,000 FMR
    - Provide estimates of system stability to race, and gender.