U.S. Department of Homeland Security

SCIENCE AND TECHNOLOGY DIRECTORATE

Remote Identity Validation Tech Demo Challenge

Science and Technology

Yevgeniy Sirotin
Identity and Data Sciences Laboratory at
the Maryland Test Facility

Arun Vemury
Senior Advisor
Biometric and Identity Technology Center
DHS Science & Technology Directorate

April 8, 2024

Outline

- Congratulations on your conditional acceptance to participate in RIVTD Track 3 as an Active Presentation Attack Detection (PAD) System

- Scenario Test Overview
- VIP Day

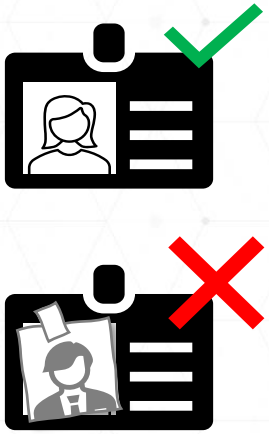
- Final Acceptance Requirements
  - Hardware & System Safety
  - Software & Application Programming Interface (API)
  - Cooperative Research and Development Agreement (CRADA) & Communication
  - System Installation at Maryland Test Facility (MdTF)

Science and Technology

RIVTD Tracks

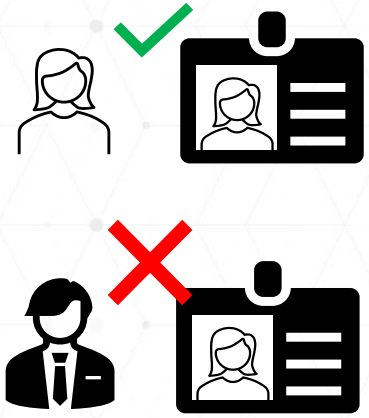
Track 1:
ID Validation

- Information Check
- Tamper Check
- Security Check



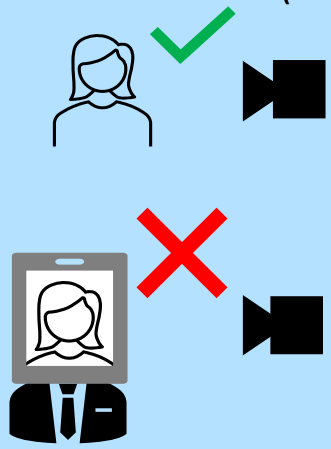
Track 2:
Match to ID

- 1:1 Verification



Track 3:
Liveness and Presentation Attack Detection (PAD)

- Reject screens and printouts
- Reject masks and other Presentation Attack (PAs)

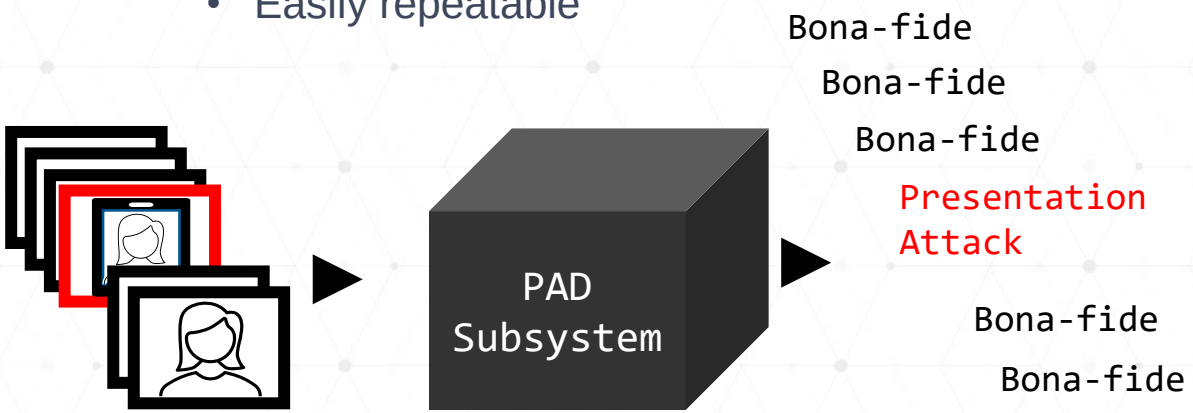


Current focus is Track 3: Liveness and Presentation Attack Detection

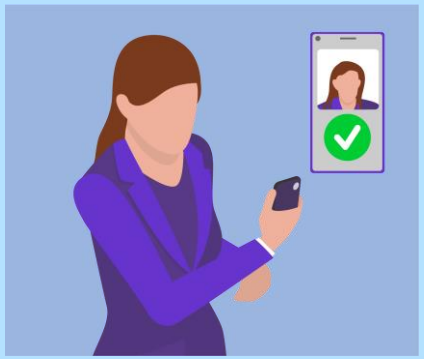
Science and Technology

Technology Tests vs. Scenario Tests

- Technology Testing:
  - Focus on performance of a multiple presentation attack detection subsystems (e.g., bona fide biometric samples, masks, replay videos)
  - Passive PAD Subsystems
  - Easily repeatable



- Scenario Testing:
  - Assess performance of PAD application in the context of use
  - Real people interact with the system
  - Active PAD subsystems
  - Costly to repeat



PAD
Application

Active PAD systems will be tested using scenario testing.

Science and Technology

Test Requirements

- Scenario Test Logistics
- Scenario Test Station
- Scenario Test Process
- Presentation Attack Instruments

Science and Technology

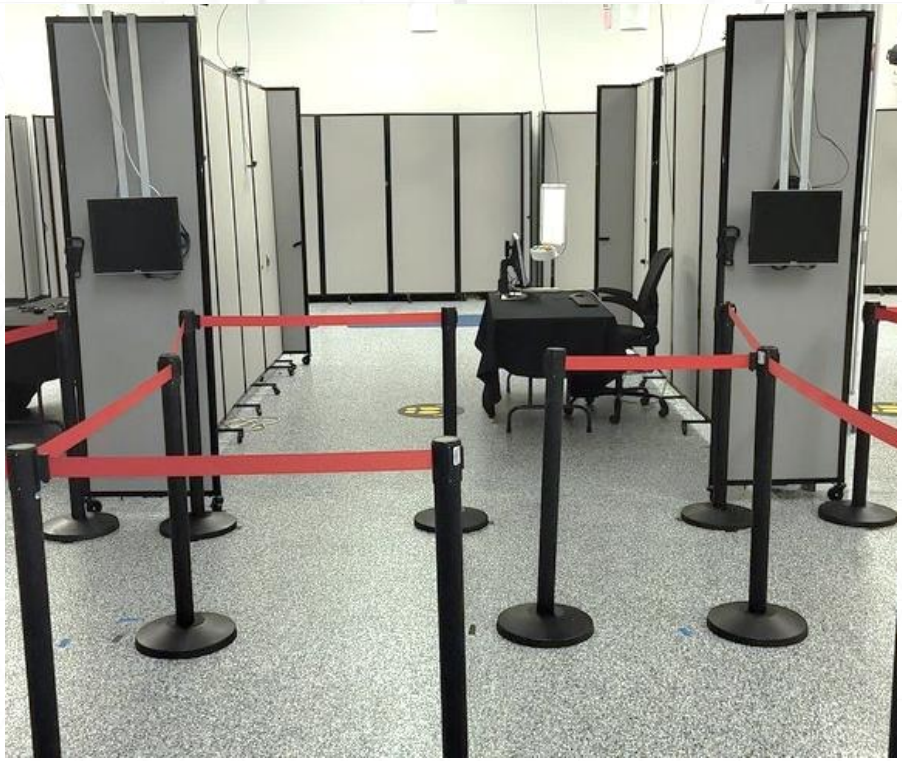
About the Maryland Test Facility (MdTF)

- Active PAD subsystems will be demonstrated at the MdTF
  - Conveniently located in Maryland near Washington DC
- Collaborator will be responsible for physically installing systems and any supporting hardware or equipment at a dedicated station
- Collaborator staff must be available remotely to address break/fix issues encountered during testing
- **No access to the internet is provided or allowed during the demonstration**

Science and Technology

Scenario Test Station

- Collaborators will be assigned a test station at MdTF
- At each station, the MdTF shall provide:
  - A 5' long table to stage collaborator PAD systems
  - A 6 outlet 120v power strip for system use
  - Network connectivity and up to **three** static IP address assignments to interface with the API backend
    - Encrypted wireless access point connectivity
    - Connectivity to one wired access point
  - A maximum current draw of up to 5 amperes (running draw)
- Collaborators shall ensure all hardware is contained within the designated station area, including any required internal system interconnectivity (cabling, switches, hubs, etc.)
- Collaborators shall ensure that a minimum 36" wide pathway for volunteers to pass through the station is maintained
- **No access to the internet is provided or allowed during the demonstration**



Science and Technology

Scenario Test Process

B MdTF Staff member starts transaction and volunteer enters station.

C MdTF Staff member provides volunteer collaborator's device with installed PAD application. Volunteer initiates and performs one **PAD transaction** using the device.

The PAD transaction may be either bona-fide or a presentation attack.

A Volunteers queue at station.

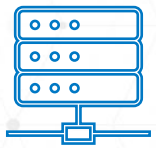
Ground Truth

Beam Break 1

Beam Break 2

Satisfaction

D Volunteer rates experience.



MdTF Server

E PAD data is sent to MdTF server.

Science and Technology

Presentation Attack Instruments

Level A	Level B	Level C
• Printout on Paper • Display on Screen	• Paper Masks • Video Replay on Screen	• Attacks requiring special hardware and significant effort/cost to perform

- The number and specific species of PAIs will not be disclosed
- PAD performance will be assessed per PAI species

System Requirements

- Active PAD System Requirements
- System Hardware & Safety
- PAD Application & API

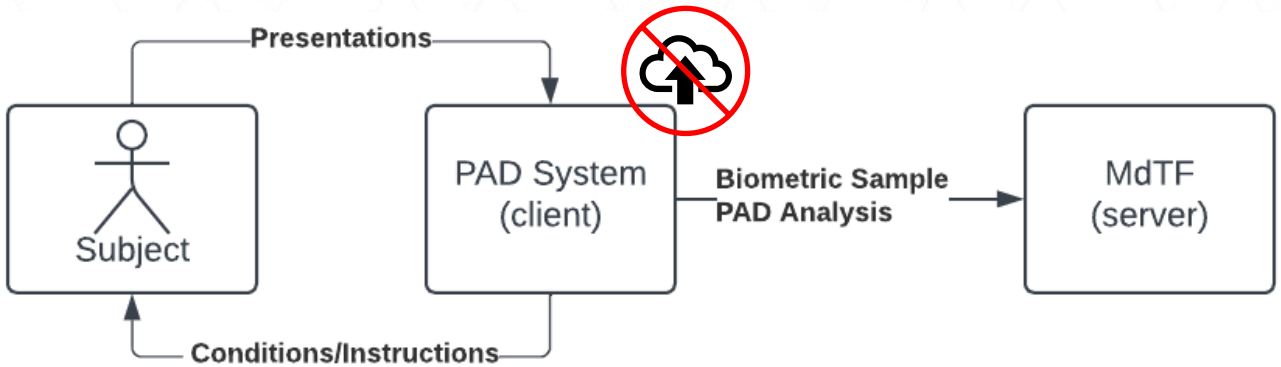
Science and Technology

Active PAD System Requirements

Science and Technology

Active PAD Subsystem Requirements (1)

- Shall be **installed by collaborator staff** in a physical test station **at the MdTF**
- Shall operate without access to the internet / cloud
  - Smartphones shall be configured to operate in “airplane mode”
- May leverage any additional compute resources installed within the test station
- Shall implement the RIVTD Active PAD subsystem API
- May instruct the subject and use standard hardware / sensors on the smartphone
- Shall cost share ($25K) with DHS S&T non-recurring engineering costs (e.g., scenario test planning, engineering, volunteer compensation)



Science and Technology

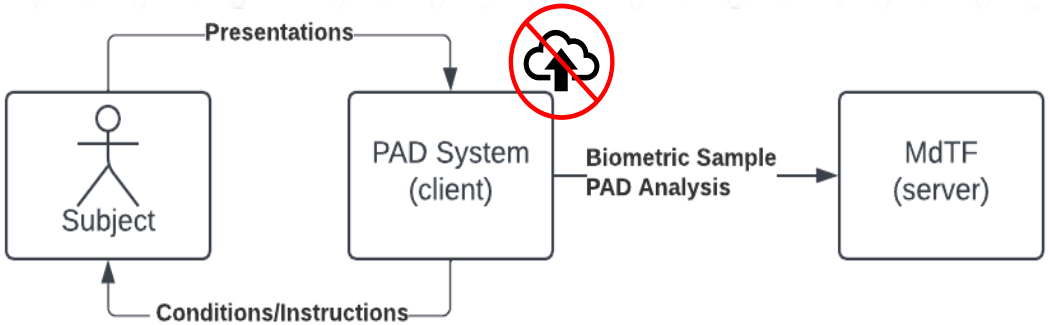
Active PAD Subsystem Requirements (2)

- Collaborator shall **provide BOTH an Android and iOS device** with the installed **PAD application** for testing
- Application shall have an interface to allow subject to initiate and complete transactions with a 30 second transaction timeout
- Application shall be able to configure “station name” and IP address of the MdTF API endpoint
- No biometric comparison is required
- Collaborator shall provide thresholds for operating points at BPCER=(1:10,1:100,1:1000,1:10000)

iPhone 14

Samsung Galaxy S22

- Shall provide the following to the MdTF server for each transaction:
  - Station ID, Mobile Platform, Biometric Sample
  - PAD Outcome: (true or false)
  - PAD Score: (0 – 1)
  - PAD Properties (key value pairs)



Science and Technology

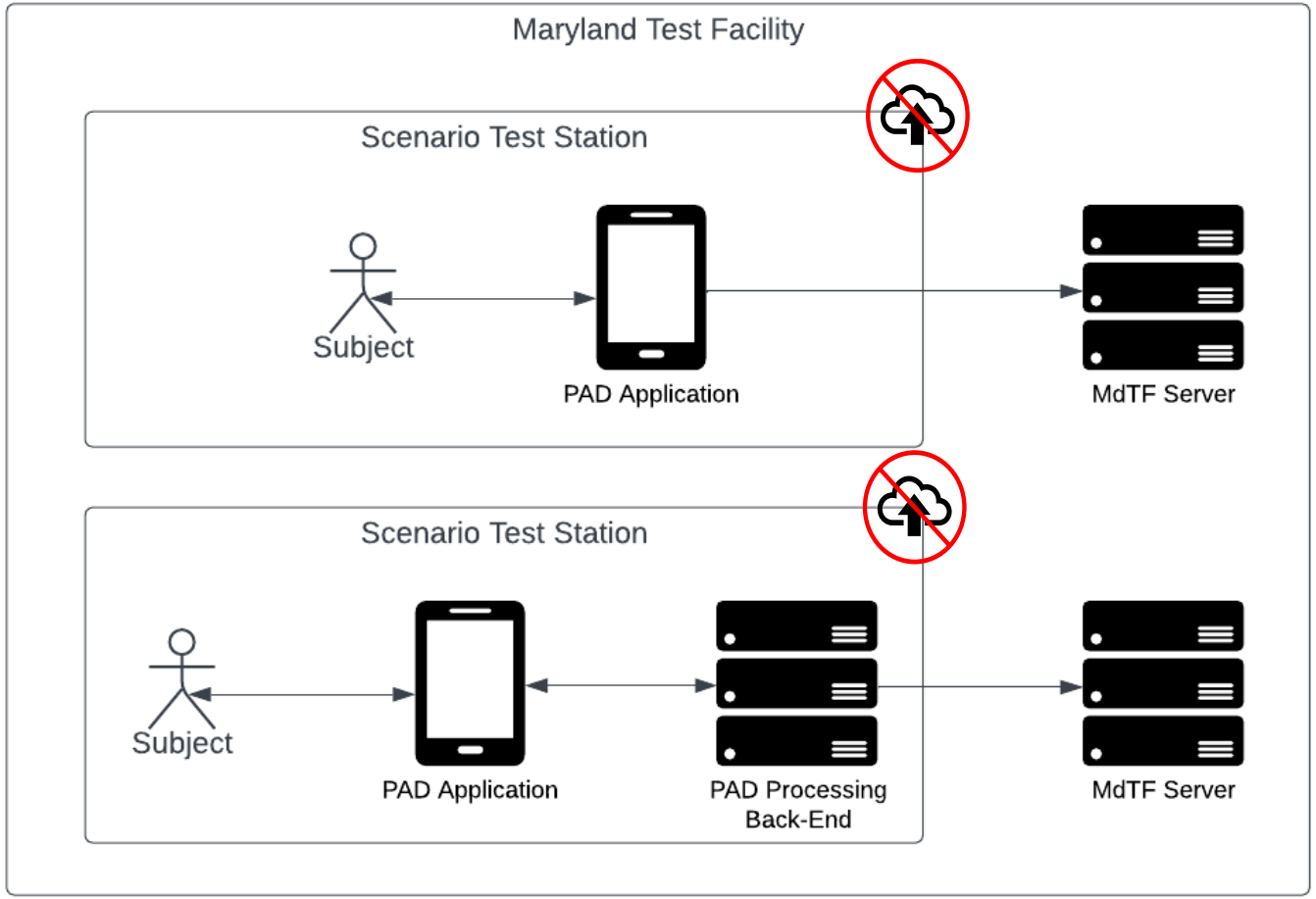
System Hardware & Safety

Hardware and System Safety

- The MdTF provides a positive, safe, and inclusive space for scenario test volunteers
  - Institutional Review Board (IRB) Requirements
  - Americans with Disabilities Act (ADA) Requirements
  - Safety Requirements
- During the scenario test volunteers will interact with collaborator-provided hardware
- To ensure volunteer safety:
  - All collaborator-provided devices shall be demonstrated as safe to the satisfaction of DHS Technical Point of Contact (POC) and MdTF staff
  - All systems shall be inspected "as installed" in their designated station to ensure:
    - Conformance with hardware requirements
    - A minimum 36" wide volunteer pathway through the station is maintained
    - No electrical, physical, or ergonomic safety concerns exist
- All conformance/safety issues shall be corrected prior to accepting the system installation for scenario testing
- Stations with outstanding conformance/safety issues will not participate in scenario testing

Sample Hardware Setup at MdTF

- Option 1:
  - All processing performed on mobile device
  - Mobile device sends results to MdTF Server
- Option 2:
  - Some processing performed on collaborator-furnished back-end server in the test station
  - Collaborator back-end server sends results to MdTF Server



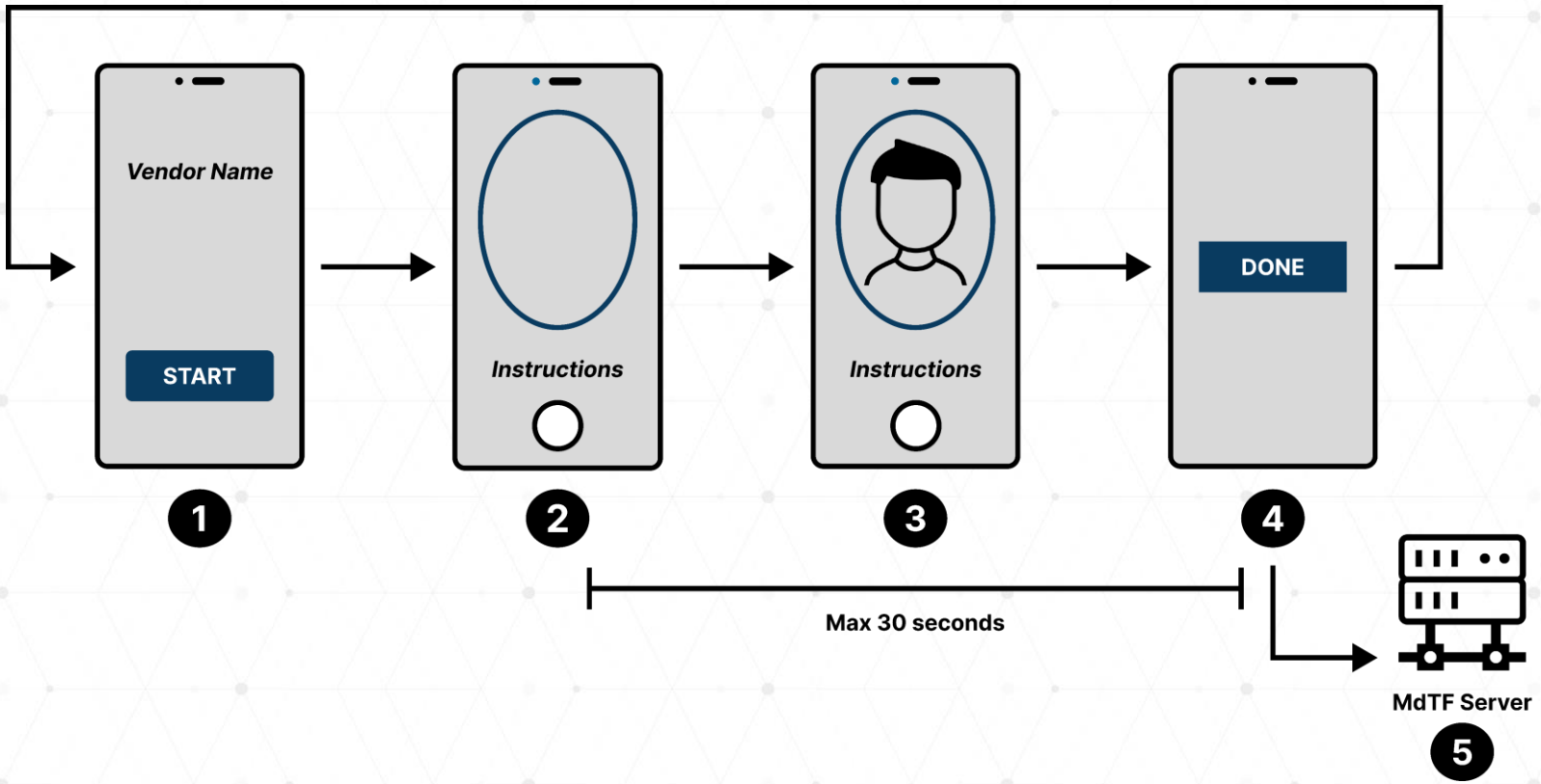
Science and Technology

PAD Application & API

Science and Technology

Sample PAD Application

1. **Home Screen**
   - Contains a button to start capture
   - Proceed to Capture (2) on tap
2. **Biometric Capture Screen**
   - Provides instructions
   - Captures a face sample using front camera
3. **Volunteer Interaction**
   - Volunteer follows instructions
4. **Done**
   - Sample Acquired and Classified → proceed to API Response (5)
   - 30 second limit reached → reset to Home Screen (1)
5. **API Response**
   - Send response to MdTF Backend
   - Reset to Home Screen (1)



Science and Technology

Active PAD API

The Maryland Test Facility Active Presentation Attack Detection System Interface

2.0.0 OAS 3.0

Data Submission

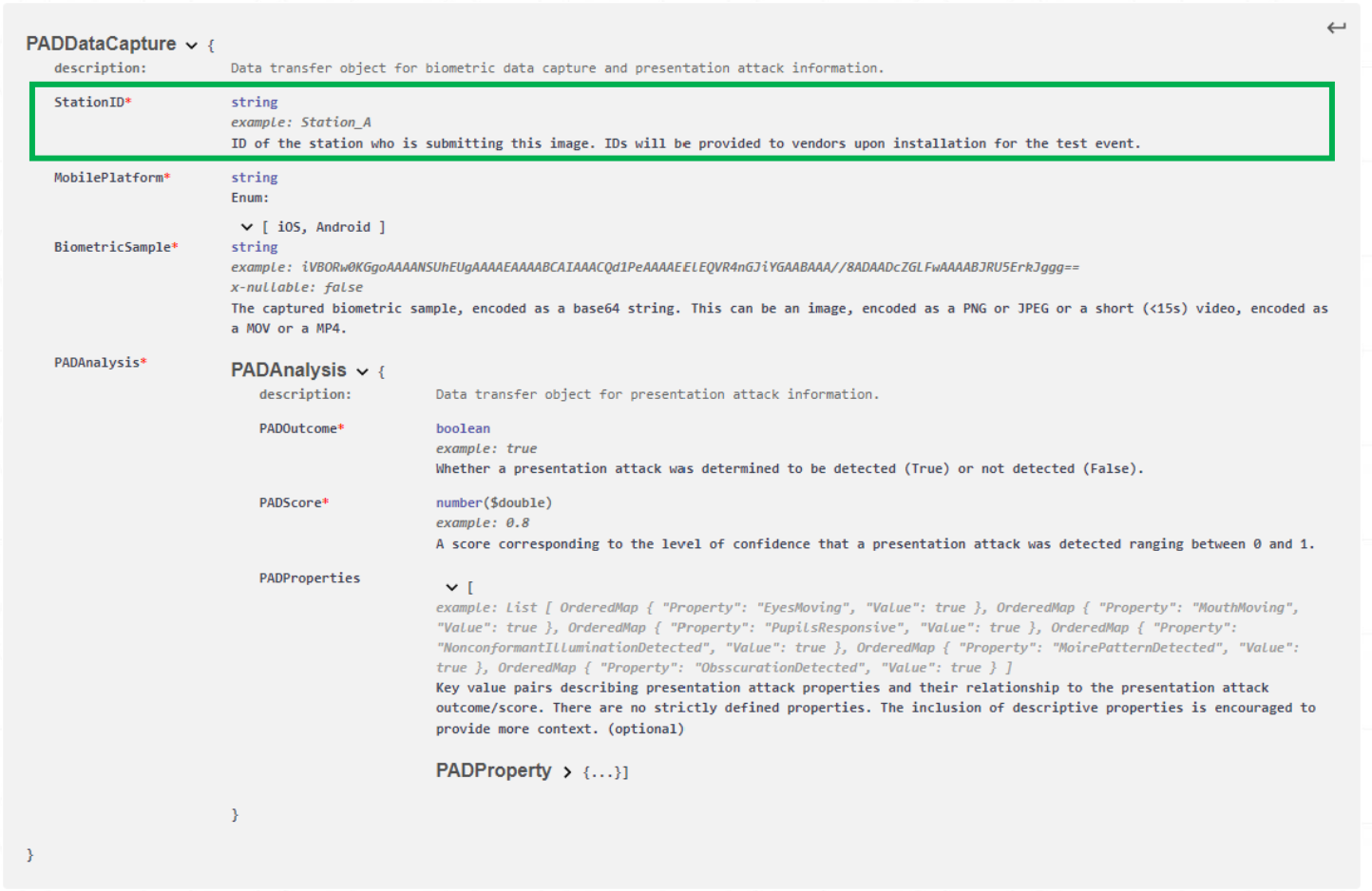
POST `/v1/capture-data-with-pad` Create a biometric data capture with associated PAD information.

- Active PAD subsystems shall send:
  - Station ID
  - Mobile Platform
  - Biometric Sample
  - PAD Outcome (true or false)
  - PAD Score (0-1)
  - PAD Properties (key value pairs)
- API Documentation is available at:
  - https://github.com/TheMdTF/mdtf-public/tree/master/apis/pad-systems

Science and Technology

Station ID

- PAD subsystems shall set their **StationID** as the MdTF-provided “station name”
  - E.g., “Station A”



PADDataCapture {

description: Data transfer object for biometric data capture and presentation attack information.

StationID* string
example: Station_A
ID of the station who is submitting this image. IDs will be provided to vendors upon installation for the test event.

MobilePlatform* string
Enum:
[iOS, Android]

BiometricSample* string
example: iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAIAAACQd1PeAAAAEElEQVR4nGJiYGAABAAA//8ADAADcZGLFwAAAABJRU5ErkJggg==
x-nullable: false
The captured biometric sample, encoded as a base64 string. This can be an image, encoded as a PNG or JPEG or a short (<15s) video, encoded as a MOV or a MP4.

PADAnalysis* PADAnalysis {

description: Data transfer object for presentation attack information.

PADOutcome* boolean
example: true
Whether a presentation attack was determined to be detected (True) or not detected (False).

PADScore* number($double)
example: 0.8
A score corresponding to the level of confidence that a presentation attack was detected ranging between 0 and 1.

PADProperties [
example: list [OrderedMap { "Property": "EyesMoving", "Value": true }, OrderedMap { "Property": "MouthMoving", "Value": true }, OrderedMap { "Property": "PupilsResponsive", "Value": true }, OrderedMap { "Property": "NonconformantIlluminationDetected", "Value": true }, OrderedMap { "Property": "MoirePatternDetected", "Value": true }, OrderedMap { "Property": "ObsscurationDetected", "Value": true }]
Key value pairs describing presentation attack properties and their relationship to the presentation attack outcome/score. There are no strictly defined properties. The inclusion of descriptive properties is encouraged to provide more context. (optional)

PADProperty > {...}]

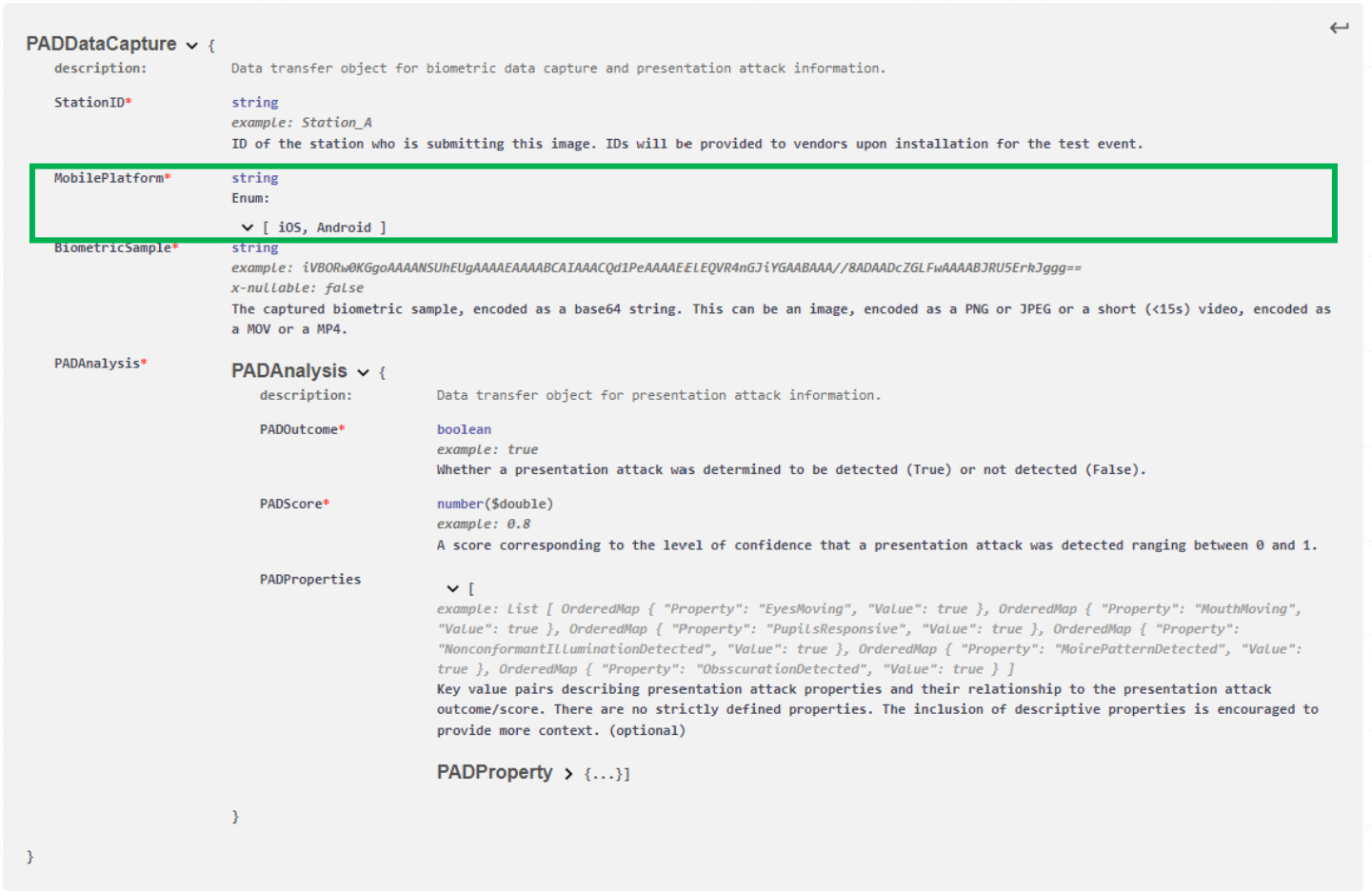
}

}

Science and Technology

Mobile Platform

- PAD subsystems shall set their **MobilePlatform** as the OS on which the system is running:
  - Active PAD systems on iPhones shall be configured to return “iOS”
  - Active PAD systems on Android phones shall be configured to return “Android”



PADDataCapture {

description: Data transfer object for biometric data capture and presentation attack information.

StationID* string
example: Station_A
ID of the station who is submitting this image. IDs will be provided to vendors upon installation for the test event.

MobilePlatform* string
Enum:
[iOS, Android]

BiometricSample* string
example: iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAIAAACQd1PeAAAAEElEQVR4nGJiYGAABAAA//8ADAADcZGLFwAAAABJRU5ErkJggg==
x-nullable: false
The captured biometric sample, encoded as a base64 string. This can be an image, encoded as a PNG or JPEG or a short (<15s) video, encoded as a MOV or a MP4.

PADAnalysis* PADAnalysis {

description: Data transfer object for presentation attack information.

PADOutcome* boolean
example: true
Whether a presentation attack was determined to be detected (True) or not detected (False).

PADScore* number($double)
example: 0.8
A score corresponding to the level of confidence that a presentation attack was detected ranging between 0 and 1.

PADProperties [
example: list [OrderedMap { "Property": "EyesMoving", "Value": true }, OrderedMap { "Property": "MouthMoving", "Value": true }, OrderedMap { "Property": "PupilsResponsive", "Value": true }, OrderedMap { "Property": "NonconformantIlluminationDetected", "Value": true }, OrderedMap { "Property": "MoirePatternDetected", "Value": true }, OrderedMap { "Property": "ObsscurationDetected", "Value": true }]
Key value pairs describing presentation attack properties and their relationship to the presentation attack outcome/score. There are no strictly defined properties. The inclusion of descriptive properties is encouraged to provide more context. (optional)

PADProperty > {...}]

}

}

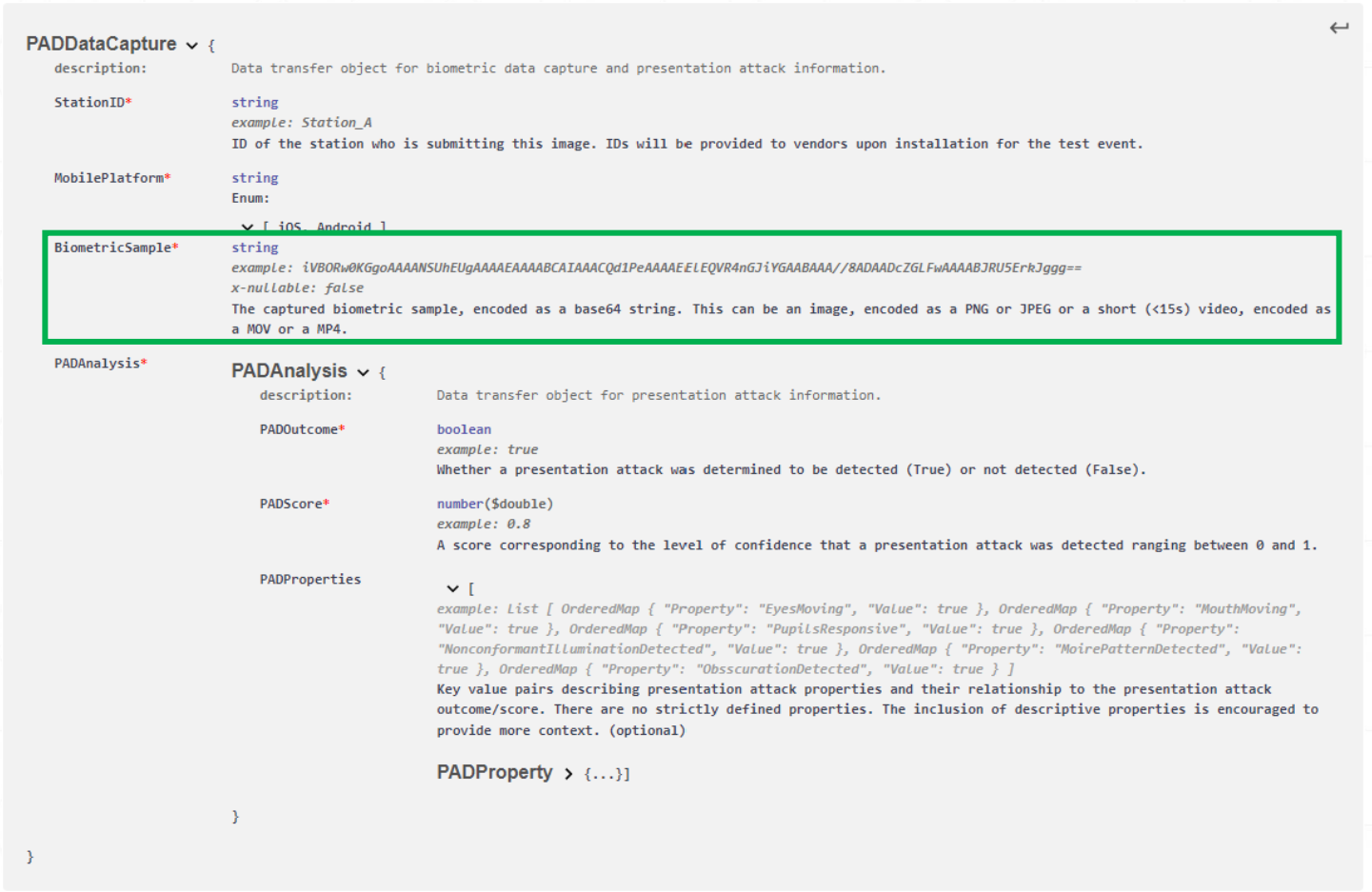
Biometric Sample

- PAD subsystems shall provide **BiometricSample** data

- The biometric sample should best represent the PAD decision:
  - If bona-fide, it's the sample that best represents the bona-fide face
  - If presentation attack, it's the sample that best represents the attack

The biometric sample can be a still image or a short video clip (<10 seconds)

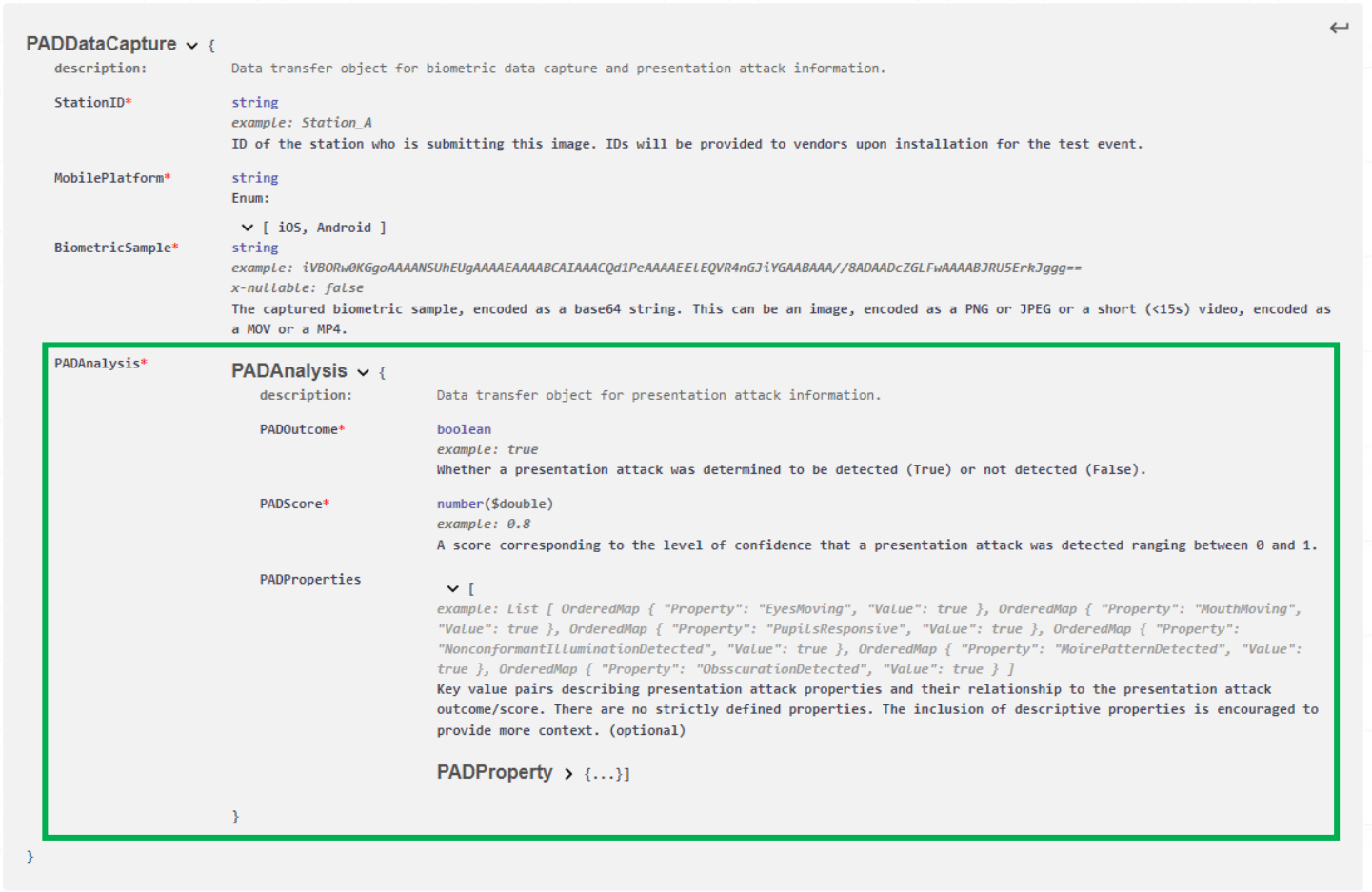
Please reach out if your media format is not supported



Science and Technology

PAD Outcome and PAD Properties

- Each **PADDataCapture** shall provide **PADAnalysis** results
- **PADOutcome** shall specify whether the biometric sample is a presentation attack (True) or a bona-fide (False)
- **PADScore** shall indicate level of confidence on whether the biometric sample is a PA:
  - 1 means 100% certain it's a PA
  - 0 means 0% certain it's a PA (i.e., its bona-fide)
- **PADProperties** are key value pairs indicating any properties used by the PAD subsystem to determine PAD outcome and the values of those properties



Science and Technology

Final Acceptance Requirements

- Staff List
- CRADA
- Communications
- API Integration
- PAD System Delivery & Installation

Science and Technology

System Provider Staff List

- PAD system providers must email a list of staff members who will participate in RIVTD Track 3 activities rivtd@mdtf.org and peoplescreening@hq.dhs.gov with the subject line of **“<Company Name> RIVTD Track 3 Staff”**

- PAD system providers additionally need to list:
  - Slack channel staff (people to be given access to Slack)
  - People that will come to the MdTF for System Installation
  - People that will provide remote break/fix support for the PAD system
  - People that will come to the MdTF for the RIVTD Track 3 VIP Day
    - Include citizenship information for people that will come to the MdTF

- List due by 10am ET **April 15, 2024**

Science and Technology

Slack Channel Access

- Identify up to three (3) individuals from your company to serve as **Slack Channel Staff** to communicate with the MdTF Technical team

- Technical POC should send the list to rivtd@mdtf.org with the subject line of **"<Company Name> RIVTD Track 3 Slack Channel Staff"**
  - **To ensure timely access, this list is due by 10am ET April 19, 2024**

- Each **Slack Channel Staff** must email rivtd@mdtf.org with the subject line of **"<Company Name> RIVTD Track 3 Account Request"**

- Originating e-mail must be listed in a prior e-mail from the technical POC

Cooperative Research and Development Agreement (CRADA)

- Agreement between each System Provider (COLLABORATOR) and DHS S&T (SPONSOR)
  - Defines the roles and contributions of the COLLABORATOR and SPONSOR
  - Provides the basis for involvement in RIVTD Track 3 activities
  - Exempt from Freedom of Information Act (FOIA) process

- Must be signed by Corporate Officer

- Submission instructions will be provided when the CRADA is emailed. Signed CRADA is due by 10am ET **April 26, 2024**

PAD System API Integration

- PAD system providers are required to demonstrate that they have integrated their system with the MdTF Active PAD API
  - http://github.mdtf.org

- PAD systems shall demonstrate API integration by submitting a PADDataCapture to the appropriate endpoint
  - NOTE: the location of this API endpoint will need to be re-configured at MdTF

- Email rivtd@mdtf.org once a PADDataCapture has been submitted and the MdTF will verify submission. This is a prerequisite for final acceptance:
  - Deadline: 10am ET **April 26, 2024**

PAD System Delivery

- PAD system providers are responsible for getting their systems to the MdTF
  - System providers are responsible for ALL international shipment logistics, including US Customs arrangements
  - PAD system shipments will be received and staged in the assigned station 1 week prior to installation – any shipments received before **April 29, 2024** will be rejected

- Address:

  Maryland Test Facility
  1221 Caraway Court, Suite 1070
  Upper Marlboro, MD 20774
  Attn: Colette Bryant (301) 909 - 9300

- Please label all packages with your company name and appropriate POC

- PAD system providers will be responsible for return shipping
  - Scenario testing may continue through **August 30, 2024**

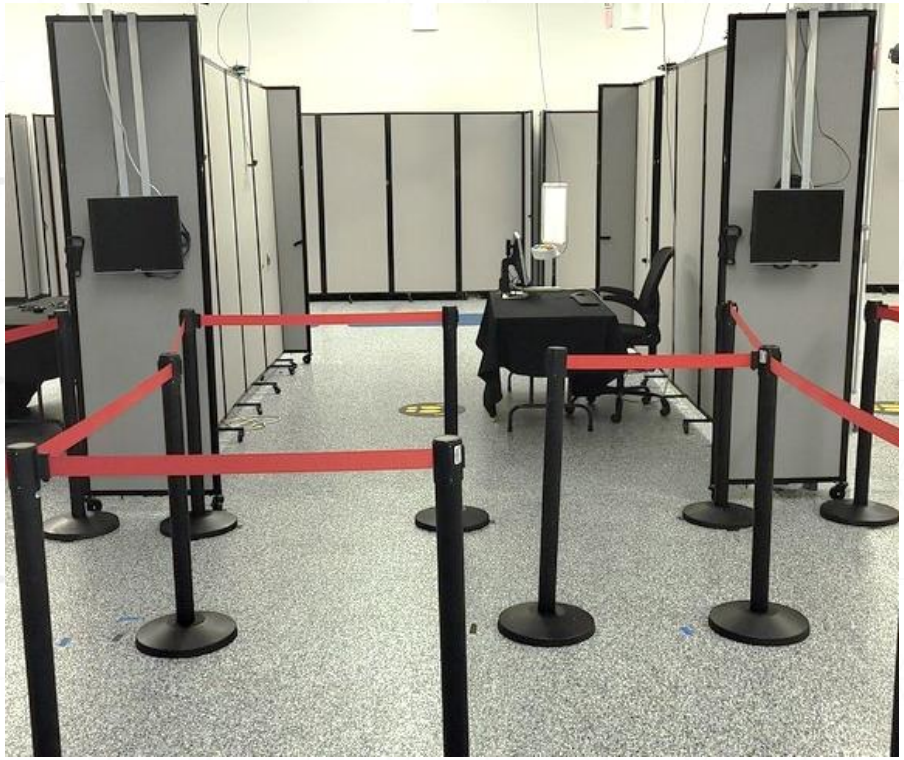
PAD System Installation

- PAD system providers are responsible for getting all required hardware to the MdTF

- There will be multiple stations at the MdTF, each labelled with a letter
  - You will be assigned to one of these stations upon arrival (e.g., “Station A”)

- PAD system provider shall configure:
  - Up to three MdTF assigned static IP addresses for their systems
  - The IP address of the Active PAD API endpoint
  - Their “station name” to use for API requests

- There will only be ONE (1) day for system installation, **May 6, 2024**



The Active PAD API endpoint will be different from the endpoint used for demonstrating API integration

Science and Technology

After Installation

- VIP Day
- Break/Fix Support

Science and Technology

VIP Day

- VIP day will be held at MdTF on **May 7, 2024**
- VIP day is an opportunity for your organization to pitch your system to stakeholders from DHS, other federal and international government agencies, and various trade associations that may attend
- VIPs will be divided into groups that will visit each collaborator station
- You will have ~10 minutes with each VIP group to demonstrate and promote your system
- You may also bring materials, such as promotional posters, to set up in your station
  - All promotional materials must fit within your station and must be removed following VIP day
- You may bring up to **three** personnel to the MdTF on VIP day, as long as you have provided the required information for those personnel to come to the MdTF
  - Non-USCs must be cleared by DHS in advance, names needed by 10am ET **April 15, 2024**

Break / Fix Support

- System provider shall make staff available and will be solely responsible for addressing any break/fix issues encountered with their system during testing
- The MdTF will provide internet connectivity to handle break/fix interventions remotely when testing is not being performed
- Scenario testing will be carried out between **May 8, 2024** and **August 30, 2024**
- Intensive testing is expected between **May 8, 2024** and **May 24, 2024**
- System breakdowns during testing may result in missing data from scenario test transactions and missing data will be treated as a system error
- Failing to address system issues will result in lower measured system performance

Resources & Where to Ask Questions

- A detailed Statement of Work (SOW) will be provided in the CRADA
- All legal and logistics questions should be directed to peoplescreening@hq.dhs.gov
- Technical communication pertaining to RIVTD Track 3 should be handled via Slack (chatroom):
  - API Integration and Implementation, Metrics
- Technical questions can be sent to rivtd@mdtf.org, but Slack is preferred
- These slides will be available on http://mdtf.org/rivtd