

MOBILE FINGERPRINTING INNOVATION TECHNOLOGY



The Mobile Fingerprinting Innovation Technology Challenge

*Advancing Mobile Fingerprint Capture Technology for
Law Enforcement*

Hosted by



PUBLIC SAFETY
COMMUNICATIONS
RESEARCH

Table of Contents

Introduction.....	1
Overview.....	1
Challenge Background.....	2
Technology Gaps	2
Observed Collection Issues with Contactless Fingerprint Capture.....	4
Challenge Goals and Objectives	4
Challenge Phases	5
Summary of Prizes	5
Important Dates.....	6
Official Contact Information.....	6
Phase 1 – Concept Paper.....	6
How to Enter.....	7
Submission Requirements.....	7
A. Cover Page and Abstract	7
B. Project Description	7
C. Information about Key Team Members	8
Evaluation Criteria and Judging.....	9
Criterion 0: Compliance Check (pass/fail)	9
Criterion 1: Strategic Alignment & Technical Outcome (70%)	9
Criterion 2: Feasibility & Team (30%).....	9
Scoring for Concept Papers	10
Phase 2 - Virtual Demonstration, Evaluation of Prototypes, and Open Source Contest	10
Walk-On Contestant Option:	10
Phase 2 Kickoff Webinar	10
How to Enter.....	11
Submission Requirements.....	11
Video Requirements.....	12
Evaluation Criteria and Judging.....	12
Evaluation of Walk-on Contestants’ Submissions.....	12
Criterion 0: Basic Compliance (Pass/Fail).....	12
Criterion 1: Demonstration Video Review (100%)	12

Evaluation of All Phase 2 Submissions	13
Criterion 0: Compliance Testing (Pass/Fail).....	13
Criterion 1: Efficiency and Effectiveness (60%)	13
Criterion 2: Feasibility (15%)	14
Criterion 3: User Satisfaction and Ease of Use (15%).....	14
Criterion 4: Innovation and Creativity (10%).....	14
Scoring for Demonstration and Evaluation of Prototypes	14
Final Prize Award Evaluation	14
Optional Prizes.....	14
Evaluation for the First Responder’s Choice Award	15
Evaluation for the Innovation Prizes.....	15
Evaluation for the Open Source Prizes	15
General Submission Requirements for All Phases (Rights & Warranties).....	15
Eligibility Requirements	15
General Eligibility Requirements	17
Special Eligibility Requirements	18
Official Representative	18
Judging Panel	19
Tie-Breaking	19
Notification and Verification of Potential Winners:.....	19
Winners Not Eligible for Cash Prizes:.....	20
No Endorsement.....	20
Submission Rights	20
Warranties	21
No Confidential Information.....	22
Additional Terms and Conditions	22
Challenge Subject to Applicable Law.....	22
Resolution of Disputes	23
Publicity	23
Payments	23
Liability and Insurance	24
Records Retention and FOIA.....	24

Privacy Advisory	24
508 Compliance	24
General Conditions	25
Appendix A: References and Resources	26
References	26
Additional Resources	26

Introduction

Overview

The Public Safety Communications Research (PSCR) Division of the National Institute of Standards and Technology (NIST) is hosting the Mobile Fingerprinting Innovation Technology Challenge (mFIT Challenge) to advance mobile fingerprint capture technologies by building and demonstrating prototype applications and/or mobile device accessories for fingerprint capture by law enforcement officers in the field. In this two-phase challenge, NIST will award cash prizes of up to \$430,000 to the winning contestants. The First Responders Network Authority and AT&T Corporation are partnering with PSCR on this challenge.

Identity verification is essential for firearm licensing, criminal background checks, employment eligibility, and protecting vulnerable populations. In addition, law enforcement personnel often encounter individuals in situations when the confirmation of the persons' identity or a background check is necessary. If the individual does not have proper identification or is possibly using a false identity, officers can capture fingerprint images and compare the images to national, state, or local identity databases to help determine the individual's identity. This information can help the officer make a better decision on whether to release the individual or hold them for further processing.

In a typical situation where a law enforcement officer needs to run a full identification check with fingerprint search, the law enforcement officer would possibly need to transport the individual to a facility for processing. Fingerprint images are critical because fingerprint data can be extremely helpful in the proper identification of an individual. However, shortages in personnel and equipment resources, as well as health and environmental factors, limit the ability of law enforcement to process and transport individuals to fingerprinting facilities.

Developing or improving fingerprint capture solutions that are more convenient and cost effective for use by field officers would minimize the financial and logistical burden on public safety organizations while ensuring officers have access to relevant identification databases. This challenge aims to create or improve an application on a mobile device, such as a smartphone or tablet, that accesses the device sensors and captures and processes high-quality digital fingerprint images that are interoperable with existing fingerprint management systems. Solutions may use contactless, contact-based, or a combination of technologies.

Continue reading to learn about the challenge phases, important dates, submission requirements and evaluation criteria.

Challenge Background

Today, there are commercially available, certified hardware peripheral devices (i.e., listed on *Appendix F* of the FBI Electronic Biometric Transmission Specification (EBTS)) that law enforcement personnel use for the purposes described that are highly accurate, meet current standards, and are interoperable with fingerprint databases. These devices tend to be portable and are mostly connected to smartphones, tablets, or laptops via cable or wireless communications to transfer files. The files may be stored, managed, or manipulated by a mobile application on a smartphone or tablet. However, these devices require agencies to purchase additional equipment and field officers to carry that equipment in addition to the large collection of equipment they already carry. While these are technically mobile devices, the term “mobile device” for the purposes of this challenge and throughout these Official Rules means a smartphone or tablet from a major vendor that can run mobile applications and access the available device sensors to capture digital fingerprint images. The use of existing or modified certified hardware peripheral devices [1] is not permitted in this challenge.

The focus of this challenge is to build on current mobile fingerprint technologies or develop new technologies that are more efficient and cost effective than what is currently available. This technology will allow law enforcement officers to capture digital fingerprint data necessary to identify an individual who may not have proper identification without the officer having to carry additional equipment or transport an individual to a fingerprinting facility. This challenge asks contestants to submit a mobile application that captures quality digital images of at least two fingers (including index and middle) on the left and right hands.

We offer several documents to assist contestants with understanding the goals of this challenge, for which a reference list is offered at the end of this document. Note that this Official Rules document does not provide a detailed explanation of all characteristics of quality digital fingerprint images. We expect contestants to possess or gain that knowledge.

Technology Gaps

This challenge encourages contestants to provide innovative solutions that support the unique requirements of law enforcement officers. In preparation for this challenge, PSCR worked with multiple subject matter experts (SMEs) to understand the current state of the technology and identify technical gaps or barriers that are inhibiting advances in capturing digital fingerprints on mobile devices. While contestants are encouraged to bridge these gaps, contestants are also encouraged to explore and innovate in any area that would improve the accuracy and quality of the fingerprint capture technology. The SMEs identified the following technology gaps:

Technology Gap #1: Accurately measuring distance

Accurate contactless fingerprint capture requires knowing the precise distance from the camera to the finger. Utilization of a device’s onboard sensors such as the video camera and distance meter (e.g., Time of Flight or LIDAR) may be used to aid in accurate fingerprint capture. Code that utilizes these sensors could provide the ability to capture necessary image detail.

Technology Gap #2: Flatten a distorted image and identify distortion

Distortion based on finger pose and shape degrades the usability of fingerprints for accurate matching. Photometric distortion causes missing areas and spurious minutiae points, while geometric distortion manipulates the spatial location of features. Image processing algorithms could be used to establish the pose and position of the hand and fingers to improve optical recognition.

Technology Gap #3: Improve the efficiency of rendering algorithms

Algorithms used for the rendering of images from mobile device sensors can be computationally intense, and novel solutions could increase this complexity. New methodologies and algorithm improvements can enable rendering using the modest computation capability of mobile devices.

Technology Gap #4: Accessing available sensors on mobile devices

Modern mobile devices feature several sensors such as high-resolution and high-speed CMOS (complementary metal oxide semiconductor) image sensors, a GPS sensor, accelerometer, gyroscope, magnetometer, ambient light sensor, microphone, distance measuring sensors, and fingerprint sensor [2]. Contestants are encouraged to use available sensors on a mobile device that will improve the quality of fingerprint images. Another sensor available on some devices is an ultrasonic fingerprint scanning sensor; however, this device sensor is currently only used for smartphone authentication purposes and is not available to 3rd party applications. The potential for the use of ultrasonic fingerprint scanning sensors is demonstrated by Qualcomm's device certified by the FBI EBTS [3]. While this device was specially engineered for use by the Department of Defense and is a different form factor than smartphones and tablets, it demonstrates the use of ultrasonic technology in capturing quality digital fingerprint images.

Technology Gap #5: Sensors that have the potential to be included on mobile devices

The mFIT Challenge will allow the addition of sensors that are not currently available on mobile devices but have the potential to be made available in the future. These sensors can be added to the contestants' submitted devices but will be evaluated and scored based on the realistic potential that they could be included in future, commercially available mobile devices. This evaluation and scoring will include criteria such as cost to implement, impact on form factor, ruggedness for use by law enforcement, and potential for technological advances on these sensors that will reduce cost and improve form factor. The intent is to retain the basic form factor of the mobile device so an officer does not need to carry a peripheral device.

Technology Gap #6: Modifications to the mobile device or the use of add-on components

Contestants may make small changes to the form factor of a mobile device to improve how the sensors function or add new functionality. An example of this type of change is a lens overlay that changes the functionality of the camera. Mobile device cases or skins that include such add-on components are allowed. Any use of add-on components will be evaluated and scored based on the realistic potential that they could be attached or implemented on a mobile device. This evaluation and scoring will include criteria such as cost to implement, impact on form factor, ruggedness for use by law enforcement, and potential for technological advances on these

components that will reduce cost and improve form factor. The intent is to retain the basic form factor of the mobile device so an officer does not need to carry a peripheral device.

Observed Collection Issues with Contactless Fingerprint Capture

The following major issues, as cited in [NIST.SP 500-334](#), should be considered for any contactless fingerprint capture technologies. Note that contactless capture is only one potential set of technologies appropriate for this challenge, and contact-based capture may also succeed in this challenge.

Motion Stability: For portable capture devices, the motion of the device or the subject can negatively impact capture. The most challenging scenario encountered was a moving/unstable capture device coupled with a moving/unstable subject.

Background motion stability: Portable devices appeared to have more difficulty completing their collection where the background of the hand(s) comprised of moving objects or people.

Background uniformity: Noisy backgrounds (patterned imagery) impacted capture speed and success of portable capture devices.

Background contrast: Having insufficient optical contrast between the subject's hands and background negatively impacted the ability to perform the capture.

Errant lighting: Errant light sources and light noise into the capture device (portable or stationary) negatively impacted capture ability.

Inadequately Bounded Capture Volume: Having a spatially unconstrained environment caused capture difficulties with the subject moving out of the field of capture or optimal focal range.

Challenge Goals and Objectives

This challenge seeks innovative new or improved mobile applications that access the available sensors on mobile devices to capture high-quality digital fingerprint images, thereby improving the performance and efficiency of identification in the field. Contestants are asked to submit a mobile application that captures quality digital images of at least two fingers (including index and middle) on the left and right hands. The ultimate objective of this challenge is to advance technology while preserving the form factor of the mobile device. Law enforcement officers explicitly do not want to carry additional equipment; however, a contestant's prototype may modify the form factor with justification.

Challenge Phases

Phase	Phase Description	Evaluation Criteria Summary	Number of Contestants Eligible to Compete
1	Concept Paper	Compliance (Pass/Fail) Strategic Alignment & Technical Outcome (70%) Feasibility & Team (30%)	Open to all eligible Contestants
2	Virtual Demonstration, Evaluation of Prototypes, and Open Source Contest	Evaluation of Walk-on entries for Phase 2 eligibility Compliance (Pass/Fail) Efficiency and Effectiveness (60%) Feasibility (15%) User Satisfaction and Ease of Use (15%) Innovation and Creativity (10%)	Up to 5 eligible Walk-on Contestants Plus up to 15 Contestants invited from Phase 1

Summary of Prizes

The prize purse for the mFIT Challenge is up to \$430,000.

Phase	Submissions	Awards
Phase 1 – Concept Paper	Contestants will submit a concept design for their proposed solution along with team biographies.	Up to 15 teams will be awarded an invitation to Phase 2 and an \$8,500 cash prize. Total prize purse up to \$127,500
Phase 2 – Virtual Demonstration, Evaluation of Prototypes, and Open Source Contest	Contestants will develop a prototype and/or application, deliver any hardware devices/add-ons and/or software to PSCR, and provide a recorded demonstration of their proposed solution.	1 st place cash prize: \$100,000; 2 nd place cash prize: \$60,000; 3 rd place cash prize: \$30,000; First Responder’s Choice Award: \$12,500 Innovation Prizes: Up to 5 Innovation Prize Winners may win \$4,000 each for outstanding innovation. Open Source Awards: Up to 10 Open Source awards of \$8,000 each will be made to participants who

		<p>share their full source code and/or complete device specifications in a public repository.</p> <p>Total prize purse up to \$302,500</p>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------

Important Dates

Date	Event
September 16, 2021	mFIT Challenge is open for Phase 1 Concept Paper submissions
September 22, 2021	Phase 1 Kickoff Webinar
October 18, 2021	mFIT Challenge Phase 1 closes on this date at 5:00 PM (EDT) for Concept Paper submissions
November 10, 2021	Phase 1 Winners announced; begin Phase 2
November 17, 2021	Phase 2 Kickoff Webinar
March 14, 2022	Walk-on contestants and Phase 1 Winners send their letters of intent to enter Phase 2 of this challenge
April 4, 2022	<ul style="list-style-type: none"> Contestants ship prototypes for receipt at NIST PSCR by this date. Contestants upload digital materials to the designated cloud storage environment by this date at 11:59 PM (EDT). Contestants who choose to compete for an Open Source Award upload the URL of the repository containing their open-sourced code and/or device specifications and license by this date at 11:59 PM (EDT).
May 4, 2022	Phase 2 Winners announced

Official Contact Information

Questions about this Challenge should be directed to mfitprize@sensisagency.com.

Phase 1 – Concept Paper

NIST PSCR invites all eligible contestants to submit concept papers; the judging panel will evaluate their proposed approach to ensure they demonstrate a clear understanding of the problem and the objective to successfully capture a high-quality digitized fingerprint using an application on a mobile device.

Up to 15 teams will be awarded \$8,500 and an invitation to Phase 2.

How to Enter

Review these Official Rules and submit a concept paper through the mFIT Challenge website. The concept paper must be a PDF file with a **maximum of 13 pages and a file size of less than 25MB**.

- Register for the mFIT Challenge by completing the online registration form on the mFIT Challenge website, <https://www.mfitprize.com/>.
- Review the NIST-PSCR provided resources on the “Resources” tab on the mFIT Challenge website.
- Submit entries by the date provided in the Important Dates section of this document.

Submission Requirements

A. Cover Page and Abstract

Page limit: one page maximum

The cover page must include:

- Contestant’s Name or Team Name (Team, Organization or Entity Name with a complete list of individual team members)
- Contestant’s Location (City, State/Region, and Country). If Team, Organization or Entity, must include the principal place of business
- Team Logo
- Official Representative and their preferred contact information (including email, phone, and physical mailing address)
- A brief description (500 words maximum) of the unique aspects of the contestant’s approach and the potential impact that the proposed approach could have in achieving the goals of the mFIT Challenge. Do not include proprietary or sensitive information in this summary.

B. Project Description

Page limit: 10 pages maximum

The scoring criteria should be your primary objective; therefore, create your concept paper to address the criteria. Address the following points:

- Solutions need to address the use case scenario of a law officer in the field who is unable to positively identify a person; so, the officer captures a digital fingerprint using a mobile device.
- Describe how the proposed method improves the accuracy of digital fingerprint capture using applications on mobile devices that use sensors and/or add-on components to capture quality digital fingerprint images.
- Explain how the solution addresses the technology gaps listed in these Official Rules or other innovation gaps in this technology space.

- Explain how the solution addresses the unique needs of a law enforcement officer operating in various environmental conditions.
- Explain the use of current mobile sensors, new mobile sensors, add-on components or modifications (explained in this document as technical gaps 4, 5, 6) and how they are used to improve the quality and interoperability of the solution. Include an explanation of how any new sensors or add-on components will not change the form factor of a mobile device or explain the potential for improvements that will accommodate the form factor of a mobile device in the future.
- Explain the full procedure of capturing and processing fingerprint images to include:
 - Describe the process of capturing the fingerprint image, the special considerations for how that image is captured, and any safety considerations for law enforcement officers.
 - Explain all sensors used. Explain relevant details for each sensor involved and how each contributes to the quality of the processed result file.
 - Explain the process for rendering raw data from sensors and converting the image to a final .png format digital fingerprint image file with 500 pixels per inch resolution.
- Explain the design of the solution and justification for major design choices.
- Describe the competitive advantage offered by the contestant's approach or solution.
- Ensure the concept paper addresses these key requirements for integrating mobile fingerprint capture systems on smart devices:
 - Potential matching accuracy against baseline images
 - Ease of use for law enforcement personnel
 - Strategy for labeling, transferring, and storing files of captured fingerprint images
 - User-friendly design – address the unique conditions where a law enforcement officer would use this technology and how the solution accommodates those conditions.

C. Information about Key Team Members

Page limit: two pages maximum

Include information on the key team members and why they are well-suited to accomplish the project, with supporting information on their qualifications, skills and capabilities (i.e., previous projects, experience) as they relate to the mFIT Challenge goals.

NIST will review each contestant's entry in the Concept Paper phase. A submission that fails to meet the compliance criteria will be disqualified and will be ineligible to compete in this phase. Submissions that pass the initial compliance review will be evaluated and scored by a panel of judges. NIST makes an independent assessment of each concept paper based on the scoring criteria outlined below. Do not include sensitive materials in the concept paper, for example, personally identifiable information like social security numbers, business-sensitive information, tax identification numbers, etc.

Subject Matter Expert (SME): An expert in their respective field, either from NIST or from an entity collaborating with PSCR. Subject matter experts will conduct independent reviews of the

submissions received during the mFIT Challenge. The subject matter experts are not judges and, as such, will provide recommendations based on the evaluation criteria to the judging panel.

Judging panel: The Director of NIST will select members from the public safety industry, first responders, and PSCR to evaluate the submissions for the mFIT Challenge. The judging panel will take subject matter expert recommendations into consideration when evaluating contestants' submissions. The judging panel will make the final determination of awards for the mFIT Challenge.

Evaluation Criteria and Judging

Judges will evaluate the concept papers using the following criteria:

Criterion 0: Compliance Check (pass/fail)

This criterion will be evaluated on the following factor:

- Completeness according to the 'How to Enter' section

If a submission passes Criterion 0, it will be evaluated on the following criteria.

Criterion 1: Strategic Alignment & Technical Outcome (70%)

This criterion involves consideration of the following factors:

- Strategic Alignment – The extent to which the proposed approach meets the objectives listed in the mFIT Challenge goals; the likelihood the contestant's solution, if successfully implemented, will have a significant real-world impact on mobile fingerprint capture capabilities.
 - Proposed Technology & Justification – Contestant's strategy for solving the problem statement, making technological improvements and justification for those improvements aligns with the mFIT Challenge goals.
 - Method of Acquiring Fingerprint Images – Contestant's demonstrated understanding of law enforcement requirements, limitations and use case.
 - Proposed Use of Sensors, Add-on Components and Software – Contestant's hardware or software plan (types of hardware/software platform) and how the plan aligns with the mFIT Challenge goals.
- Technical Outcome – Extent to which the proposed approach will result in significant improvement in commercially available technology and will potentially result in a technical outcome that enables considerable progress toward the mFIT Challenge goals.
 - Accuracy of the technological solution – demonstrates knowledge of the technical details of mobile fingerprint capture.

Criterion 2: Feasibility & Team (30%)

This criterion involves consideration of the following factors:

- Team – The extent to which the contestant's capability can address all aspects of the proposed project with a high chance of success, including, but not limited to, qualifications, relevant expertise, and time commitment of the contestant. Reviewers will assess: (a) the relevance of the qualifications and experience of the key staff, leadership,

and technical experts, (b) the extent the contestants' prior experience and the quality of the results in similar projects related to the purpose, scope or tasks of this challenge.

- Approach – Contestant's plan to manage the limited schedule, resources, project risks, and other challenges and produce high-quality project outcomes to meet the mFIT Challenge goals.

Scoring for Concept Papers

The concept papers will be evaluated based on the criteria above. Each concept paper will be reviewed by subject matter experts and evaluated by a panel of judges. Each submission will be scored as follows: criterion 1 will be recorded on a scale of 0 to 70 points, and criterion 2 will be recorded on a scale of 0 to 30 points. Contestants will not be provided oral or written feedback based on the evaluation of their submissions. Up to 15 teams will be awarded an invitation to Phase 2 and an \$8,500 cash prize.

Phase 2 - Virtual Demonstration, Evaluation of Prototypes, and Open Source Contest

During this final phase of the mFIT Challenge, contestants will develop an application for a mobile device that will allow law enforcement officers to capture high-quality digital fingerprint data without the need to carry additional equipment. Contestants are asked to submit a mobile device loaded with a functioning application that captures fingerprint image files on the left and right hands (including index and middle fingers).

The judging panel will award up to 19 final awards: 1st \$100,000, 2nd \$60,000 and 3rd \$30,000, a First Responder's Choice Award of \$12,500, up to 5 Innovation Prize awards of \$4,000 each, and up to 10 Open Source contest awards of \$8,000 each.

Walk-On Contestant Option:

NIST will accept up to five Phase 2 submissions from "Walk-on" teams. Walk-on contestants are contestants who meet all eligibility requirements defined in these Official Rules. To compete in Phase 2, Walk-on contestants will submit all materials required for Phase 2. Walk-on contestants will not receive prize awards associated with Phase 1 during the Phase 2 competition.

Phase 2 Kickoff Webinar

Invited and walk-on Phase 2 contestants must attend or view a recording of the Phase 2 kickoff webinar to receive information on the objectives and timeframe of Phase 2 activities. The date of the Phase 2 kickoff webinar is provided in the Important Dates section of this document. Other items to be covered at the Phase 2 kickoff webinar include:

- Learn how to access the mFIT Challenge platform, how to submit documents and a Docker image (if applicable), and how to ship your mobile device package.
- Discussions regarding lab requirements of the Docker Container hosting contestants' Docker images and the use of internet resources versus resources accessible on the PSCR lab's private Wi-Fi network.

- Contestants will also receive training provided by mFIT Challenge partners and learn about collaboration opportunities with public safety entities.

How to Enter

Review these Official Rules and submit an entry as outlined in the sections below.

- Walk-on contestants will register for this challenge by completing the online registration form, accepting the terms and conditions of participation for entry.
- Phase 1 winners and Walk-on contestants will submit their letter of intent to enter Phase 2 of the mFIT Challenge via email to mfitprize@sensisagency.com by the date provided in the Important Dates section of this document. Contestants will include in their letter of intent a statement confirming they attended or watched the recorded Phase 2 kickoff webinar.
- All Phase 2 contestants will submit their complete entry by the date provided in the Important Dates section of this document.
- All contestants who wish to be considered for an Open Source Award must deposit the entire source code of their submission and all specifications needed to replicate hardware and related documentation into a public software repository accompanied by a permissive open source license. Contestants must provide the URL to their repository by the date provided in the Important Dates section of this document. Submission to the Open Source contest is optional and does not influence eligibility for other awards.

Submission Requirements

- Contestants must submit their mobile fingerprint application along with mobile device (including charging cable and necessary passcodes to operate the device), additional sensors and “add-on solution” components (if applicable), and instructions on how to use their solution (e.g., readme file), including an explanation of sensors and APIs used. Contestants may choose to use smartphone Hardware Development Kits (HDK) or include new sensors or add-on components and can submit their solution in this form, but will be scored on the potential to fully assemble the solution into a mobile device with a form factor that matches current mobile devices.
- The contestants must submit a document explaining: a) the technical gaps addressed, b) what technical improvements are offered by their solution, and c) an estimate of the timeline and cost for a public safety agency to implement the technology. The document is not to exceed **four pages**.
- Backend or external processing components may be used for improved processing of images. For any backend services, meaning software that needs to run external to the mobile device, please submit a ready-to-run Docker image. The evaluation lab has adequate computing resources to support the Docker image but has some limitations that will be discussed in the Phase 2 kickoff webinar.
- Contestants must submit a **demonstration video** not to exceed 20 minutes. The video shall include a recorded walk-through and voice-over demonstrating the full explanation of the solution, explain what technical gaps are addressed and what technical improvements were made. In addition, the demonstration video shall include an explanation of a law-enforcement use case and how the solution addresses it.

- All contestants shall ship prototypes and upload digital materials to a designated cloud storage environment by the date provided in the Important Dates section of this document.

Video Requirements

Section	Time Limit	Description
Overview	5 minutes	Provide a complete explanation of the solution, including the technical gaps addressed and the technical improvements made. Target audience is the general public.
Full Functionality Demonstration	15 minutes	Video demonstrating the full functionality of the prototype providing complete context. Provide as much detail as possible within the time limit. Target audience is the NIST panel of subject matter experts and judges.

Evaluation Criteria and Judging

NIST PSCR will screen submissions for completeness and compliance with the objectives and Official Rules of this contest. A submission that fails to meet the compliance criteria will be disqualified and will be ineligible to compete in this contest.

Submissions that pass the initial compliance review will be evaluated and scored by the judging panel. An evaluation of a submission by the judging panel does not constitute NIST's final determination of the contestant or submission eligibility.

Evaluation of Walk-on Contestants' Submissions

Criterion 0: Basic Compliance (Pass/Fail)

- Verification of completeness according to “How to Enter” Phase 2 requirements.

In the event there are more than five compliant Walk-on submissions, NIST will further evaluate the submissions using the following criterion.

Criterion 1: Demonstration Video Review (100%)

- The SME panel will review the demonstration videos for a clear depiction of all components of the solution, including an explanation of the solution, the technical gaps addressed, and the technical improvements made. The SME panel will provide a summary analysis to the judges.

The five highest ranked submissions, as determined by the judges, will advance to the All Phase 2 Submissions Evaluation.

Evaluation of All Phase 2 Submissions

Following the evaluation of Walk-on contestants' submissions, the SMEs and judges will continue the review and evaluation process of all Phase 2 submissions using the following criteria:

Criterion 0: Compliance Testing (Pass/Fail)

This compliance testing includes:

- Verification of completeness according to "How to Enter" Phase 2 requirements.
- Verification the devices and mobile applications are responsive to the contest.
- Evaluation of devices and mobile applications for potential safety and security risks to NIST staff, SMEs, judges, and government facilities.
- That devices and mobile applications can be operated by SMEs and judges with minimal installation and assembly.
- Verification the solution is capable of capturing quality digital images of at least two fingers (including index and middle) on the left and right hands, and the resulting digital images are in PNG file format have a resolution of 500 pixels per square inch (ppi) \pm 5 ppi. Optical resolution of devices may be higher than 500 ppi, but output images must be down sampled to 500 ppi \pm 5 ppi.
- Verification the prototypes store multiple fingerprint files which can be downloaded as a batch or compressed file package (e.g., zip file) with file names that identify finger(s), hand and subject (may use codes).

Criterion 1: Efficiency and Effectiveness (60%)

In scoring for Efficiency and Effectiveness, the solution will be evaluated on how well the solution captures a quality digital fingerprint image and how that image compares to an image captured by benchmark peripheral fingerprint devices. The benchmark devices may be commercial or non-commercial. Images captured by benchmark devices will be anonymized with respect to the device. The names of benchmark device manufacturers will not be released.

The Efficiency and Effectiveness evaluation includes:

- Comprehensiveness of contestant's solution in capturing a quality digital fingerprint image.
- The contestant's solution will be compared against the results from FBI EBTS Appendix F certified hardware peripheral devices. Digital fingerprint image files collected from contestants' prototypes will be compared to corresponding digital fingerprint image files collected from Appendix F certified devices.
- The images generated by a contestant's solution will be scored by a semi-automated algorithm that evaluates image quality (e.g., entropy and contrast) and suitability (e.g., successful automated database registration) of the image for use against an identity database.
- Solutions that are fully self-contained will score higher than solutions that require a remote server for image processing.

Criterion 2: Feasibility (15%)

In scoring for the Feasibility criterion, the judges will evaluate each solution for ease with which a public safety agency could implement the solution.

The Feasibility evaluation includes:

- cost per deployment
- ability to deploy the system within four years

Criterion 3: User Satisfaction and Ease of Use (15%)

An evaluation of the solution's responsiveness to public safety user needs including:

- Ease of use
- Speed of collection and processing
- Convenience of form factor
- User satisfaction

Criterion 4: Innovation and Creativity (10%)

An evaluation of the novel approach taken by the contestant that is an outstanding technological innovation or has the potential for exceptional impact on the public safety community. Examples include, but are not limited to, the unique use of existing device sensors, the development of new image rendering algorithms, and the creation and justification of an add-on component.

Scoring for Demonstration and Evaluation of Prototypes

Each Phase 2 submission will be scored as follows: criterion 0 is pass/fail; the submissions which fail compliance will not continue in the review process. Criterion 1 will be recorded on a scale of 0 to 60 points; criteria 2 and 3 will be recorded on a scale of 0 to 15 points; criterion 4 will be recorded on a scale of 0 to 10 points. Contestants will not be provided oral or written feedback based on the evaluation of their submissions.

Final Prize Award Evaluation

For the First, Second and Third Place awards, contestants will be evaluated using a point system. The judges will rank the aggregate scores across all Phase 2 criteria for submissions that pass Phase 2 Criterion 0 (Compliance Testing); the three highest scoring submissions from Criteria 1-4 may receive the First, Second and Third Place prizes (1st place cash prize: \$100,000; 2nd place cash prize: \$60,000; 3rd place cash prize: \$30,000). NIST reserves the right to decline to make awards or make fewer awards than anticipated.

Optional Prizes

The judging panel may award the following optional prizes:

1. **First Responder’s Choice Award:** For this optional prize award, PSCR may select one (1) Phase 2 contestant submission to receive \$12,500. The First Responder’s Choice award will recognize a contestant for their responsiveness to the needs and expectations of law enforcement first responders.
2. **Innovation Prizes:** For this optional prize award, PSCR may select up to five (5) Phase 2 contestant submissions to receive \$4,000 each for submissions demonstrating outstanding innovative advancement in mobile fingerprint capture technology for law enforcement.
3. **Open Source Prizes:** PSCR will award up to ten prizes of \$8,000 each to Phase 2 contestant submissions that are deposited into a public repository with a permissive [open-source license](#). In the repository, contestants must provide their full source code and complete device specifications with sufficient detail to replicate the submission made to the Phase 2 Prototype contest. Submission to the Open Source contest is optional and does not influence eligibility for other awards.

Evaluation for the First Responder’s Choice Award

All Phase 2 submissions that have at least 30 out of 60 points for Criterion 1 will be evaluated for this award. Criterion 3, User Satisfaction and Ease of Use, scores from judges with law enforcement experience will further determine the ranking of submissions for this award.

Evaluation for the Innovation Prizes

The innovation prizes are made at the judges’ discretion to teams who show outstanding innovation in the area of fingerprint capture. The judges’ scores for Criterion 4, Innovation and Creativity, will determine the ranking of submissions for this award.

Evaluation for the Open Source Prizes

To be considered for an Open Source award, teams must submit the URL of their software and device specification repository that contains sufficient detail to replicate their solution with an open source license by the deadline specified in the Important Dates table above. Only solutions that pass Criterion 0 will be considered. In the event there are more than 10 entries, submissions will be ranked according to the final scores from Criteria 1-4, and NIST may award the top-scoring teams. Judges will only make awards to submissions they deem to be sufficiently detailed and that serve the public interest.

General Submission Requirements for All Phases (Rights & Warranties)

Eligibility Requirements

A contestant (whether an individual, private entity, or team (“Contestant” herein)) must have registered to participate and complied with all of the requirements under Section 105 of the America COMPETES Reauthorization Act of 2010 (Pub. L. No. 111-358), as amended by Section 401 of the American Innovation and Competitiveness Act of 2016 (Pub. L. No. 114-329)

and codified in 15 U.S.C. §3719 (hereinafter “America COMPETES Act” or “15 U.S.C. §3719”) as contained herein.

A Contestant who registers or submits an entry (whether an individual, private entity, or team or anyone acting on behalf of a private entity or team) to participate in this Challenge represents that they have read, understood and agree to all terms and conditions of the Official Rules.

To be eligible to win a cash prize, a Contestant must register as an individual, private entity, or team as defined below:

- Individual: a person age 18 or older at time of entry and a U.S. citizen or permanent resident of the United States or its territories.
- Private Entity: a company, institution, or other organization that is incorporated in and maintains a primary place of business in the United States or its territories.
- Team: a group of individuals or a group of private entities, with at least one member of the team meeting the definition for either Individual or Private Entity.

Contestants not eligible for cash prizes: a contestant that enters the challenge without the ability to claim a cash prize based on the eligibility requirements above. Contestants not eligible for cash prizes must be age 18 years or older at time of entry and cannot be individuals on the denied persons list nor from entities or countries sanctioned by the United States Government.

Submission Requirements

In order for submissions to be eligible for review, recognition and award, contestants must meet the following requirements:

- Deadline - The submission must be available for evaluation by the end date noted in the "Important Dates" section of these rules.
- Each submission must be original, the work of the contestant, and must not infringe, misappropriate or otherwise violate any intellectual property rights, privacy rights, or any other rights of any person or entity.
- It is an express condition of submission and eligibility that each contestant warrants and represents that the contestant's submission is solely owned by the contestant, that the submission is wholly original with the contestant, and that no other party has any ownership rights or ownership interest in the submission. The contestant must disclose if they are subject to any obligation to assign intellectual property rights to parties other than the contestant, if the contestant is licensing or, through any other legal instrument, utilizing intellectual property of another party.
- Each contestant further represents and warrants to NIST that the submission and any use thereof by NIST shall not: (i) be defamatory or libelous in any manner toward any person, (ii) constitute or result in any misappropriation or other violation of any person's publicity rights or right of privacy, or (iii) infringe, misappropriate or otherwise violate any intellectual property rights, privacy rights or any other rights of any person or entity.
- Each submission must be in English.
- Submissions to the video evaluation of Phase 2 must be in .mp4 format.

- Eligible formats for the final evaluation of Phase 2 are mobile applications (software), mobile device peripheral hardware, and text files (e.g., .docx, .pdf).

Submissions containing any matter which, in the sole discretion of NIST, is indecent, obscene, defamatory, libelous, in bad taste, which demonstrates a lack of respect for public morals or conduct, which promotes discrimination in any form, which shows unlawful acts being performed, which is slanderous or libelous, or which adversely affects the reputation of NIST, will not be accepted, and will not be evaluated or considered for an award. NIST shall have the right to remove any content from the challenge website in its sole discretion at any time and for any reason, including, but not limited to, any online comment or posting related to the Challenge.

If NIST, in its sole discretion, finds any submission to be unacceptable, then such submission shall be deemed disqualified.

General Eligibility Requirements

For all Contestants, general eligibility requirements include:

- Contestants may not be a Federal entity or Federal employee acting within the scope of their employment.
- Contestants may not be a NIST employee.
- Non-NIST Federal employees acting in their personal capacities should consult with their respective agency ethics officials to determine whether their participation in this Challenge is permissible. A contestant shall not be deemed ineligible because the individual or entity used Federal facilities or consulted with Federal employees during this challenge if the Federal employees and facilities are made available to all contestants on an equitable basis.
- Contestants may not be a NIST contractor or associate, or private entity providing services to NIST acting within the scope of their contract, employment, or funding or acquisition agreement with NIST which would involve the use of NIST funding to support a contestant's participation in the challenge.
- Contestants may not be working with NIST as a CRADA collaborator if the CRADA provides the contestant with access to NIST information, equipment or other resources which could provide any advantage to the contestant in this challenge. Contestants understand and agree that any device or data submitted as part of this challenge is not subject to the terms of any related CRADA or other agreement between NIST and the Contestant.
- Contestants may not be individuals or private entities which provide program support services to NIST, including strategic planning, project/program management, communications, reporting, program evaluation, or other similar services to NIST.
- Individuals who are former NIST Federal Employees or NIST Associates are not eligible to enter as an individual or member of a team for 365 days from their last date of paid employment or association with NIST with the exception of individuals in a student internship, experiential learning, or similar temporary employment status.

- Any individuals (including an individual’s parent, spouse, or child) or private entities involved with the design, production, execution, distribution or evaluation of the Challenge are not eligible to enter as an individual or member of a team.
- Employees of any official co-sponsoring entities are not eligible to enter.
- A Contestant (whether participating as an individual, private entity, or member of a team) must not have been convicted of a felony criminal violation under any Federal law within the preceding 24 months and must not have any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.
- Contestants must not be suspended, debarred, or otherwise excluded from doing business with the Federal Government.

Special Eligibility Requirements

- Individuals currently receiving NIST funding through a grant or cooperative agreement are eligible to compete but may not utilize the NIST funding for competing in this challenge.
- Previous and current PSCR prize challenge contestants are eligible to enter.

Official Representative

At the time of entry, all contestants must designate one individual to serve as their Official Representative and one individual to serve as an alternate to assume the role and requirements of the Official Representative if, and only if, the first individual has resigned from their role as Official Representative or has failed to respond to NIST communications for 30 consecutive days. The Official Representative will be the only individual with authority to officially interact and communicate with NIST regarding the contestant-created materials, completion of tasks as part of the challenge, signing official documentation related to the challenge, providing information to process prize payments, and any other administrative requests related to the challenge.

The eligibility of a contestant is determined by the Contestant’s registration status (individual, private entity or team) as defined above – the Official Representative does not determine the Contestant’s eligibility.

- For Individual Contestants, by default, the Official Representative must be the individual.
- For Private Entity Contestants, the Official Representative can be any individual designated by the Private Entity.
- For a Team Contestant
 - If the Team is comprised of Individuals, the Official Representative must be a team member who individually meets the eligibility requirements of an Individual Contestant.
 - If the Team is comprised of Private Entities, the Official Representative can be any individual designated by the Private Entity leading the team.

- If the Team is comprised of a mix of Individuals and Private Entities, the Official Representative, designated by the team, can be any qualified individual meeting the requirements of an Individual or member of a Private Entity.

The Official Representative will be authorized to interact with NIST and be responsible for meeting all entry, evaluation, and administrative requirements of the challenge.

If a contestant decides to withdraw their submission from consideration, the Official Representative must notify NIST in writing of their decision.

If a contestant (whether an individual, private entity, or team) is selected as a prize winner, NIST will award a single dollar amount to the account named in the standard form 3881 (ACH Vendor/Miscellaneous Payment Enrollment Form) by the Official Representative. The named account must belong to an individual or private entity as defined above in the eligibility requirements for Individual or Private Entity.

On behalf of the team as defined above, the Official Representative shall be solely responsible for allocating any prize amount among the members of the team. NIST will not arbitrate, intervene, advise on, or resolve any matters between team members.

Judging Panel

A qualified panel of experts selected by the Director of NIST will judge the submissions. The panel consists of experts from within NIST and outside of NIST; they will evaluate the submissions according to the criteria identified above to select winners. Judges will not have personal or financial interests in, or be an employee, officer, director, or agent of any entity that is a registered contestant in a challenge; or have a familial or financial relationship with an individual who is a registered contestant. The decisions of the judging panel for the contest will be announced in accordance with the dates noted in these rules. NIST PSCR will not make evaluation results from the judging panel available to contestants or the public.

Tie-Breaking

In the event of a tie between contestants, the judges will review the evaluations of the contestant submissions to assess if there is a means based on the evaluation data to differentiate the submissions in order to break the tie. If the submissions cannot be differentiated to break the tie based on the evaluation data, the contestants shall split equally the combined prize amounts of the tie (for example, a tie for 1st place, where the 1st place prize is \$30,000 and the 2nd place prize is \$20,000 will result in the two contestants each being awarded \$25,000 (equaling $(\$30,000 + \$20,000)/2$). If this tie-breaking provision is applied, the tied contestants will share the highest-placed prize, and the next lower place prize will be “skipped” (for example, 1st, 1st, 3rd, etc.). This tie-breaking provision will be applied to all ties involving two or more contestants. In resolving all ties, the total cumulative value of prizes awarded will not change.

Notification and Verification of Potential Winners:

ALL POTENTIAL CHALLENGE WINNERS WILL BE SUBJECT TO VERIFICATION OF IDENTITY, QUALIFICATIONS AND ROLE IN THE CREATION OF THE SUBMISSION BY THE DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Contestants must comply with all terms and conditions of the Official Rules. Winning a prize is contingent upon fulfilling all requirements contained herein. The potential winners will be notified by email, telephone, or mail after the date of winning results. Each potential winner of a monetary or non-monetary award will be required to sign and return to the Department of Commerce, National Institute of Standards and Technology, within ten (10) calendar days of the date the notice is sent, an ACH Vendor/Miscellaneous Enrollment Form (OMB NO. 1510-0056) and a Contestant Eligibility Verification form in order to claim the prize.

In the sole discretion of the Department of Commerce, National Institute of Standards and Technology, a potential winner will be deemed ineligible to win if: (i) the person/entity cannot be contacted; (ii) the person/entity fails to sign and return an ACH Vendor/Miscellaneous Enrollment Form (OMB NO. 1510-0056) and a Contestant Eligibility Verification form within the required time period; (iii) the prize or prize notification is returned as undeliverable; or (iv) the submission or person/entity is disqualified for any other reason. In the event that a potential or announced winner is found to be ineligible or is disqualified for any reason, the Department of Commerce, National Institute of Standards and Technology, in their sole discretion, may award the prize to another contestant.

Winners Not Eligible for Cash Prizes:

Winners who are found to be ineligible for cash prizes may still be publicly recognized. In the event that the prize award normally allotted to the place or rank of an ineligible winner occurs, the cash prize will be awarded to the next eligible winner in the series or ranking. Throughout the challenge, winners who are ineligible for cash prizes will continue to have opportunities to have their work viewed and appreciated by stakeholders from industry, government and academic communities.

No Endorsement

You agree that nothing in these Rules grants you a right or license to use any names or logos of NIST or the Department of Commerce, or any other intellectual property or proprietary rights of NIST or the Department of Commerce or their employees or contractors.

Submission Rights

Any applicable intellectual property rights to a submission will remain with the contestant. The contestant is not granting any rights in any patents, pending patent applications, or copyrights related to the technology described in the entry. However, the contestant is granting the Department of Commerce, National Institute of Standards and Technology certain limited rights as set forth herein.

- The contestant grants to the Department of Commerce, National Institute of Standards and Technology and any parties acting on its behalf the right to review the submission, to

describe the submission in any materials created in connection with this challenge, and to screen and evaluate the submission, and to have the judges, Challenge administrators, and the designees of any of them, review the submission. The Department of Commerce, National Institute of Standards and Technology, and any Challenge Co-Sponsors, will also have the right to publicize contestant's name and, as applicable, the names of contestant's team members and/or organization which participated in the submission following the conclusion of the challenge.

- You grant to NIST, and any parties acting on NIST's behalf, the right to include your name and your company or institution name and logo (if your entry is from a company or institution) as a Contestant on the Challenge Website and in materials from NIST, and any parties acting on NIST's behalf, announcing Winners, Finalists or Contestants in the Challenge. Other than these uses or as otherwise set forth herein, you are not granting NIST any rights to your trademarks.
- The contestant grants the Department of Commerce, National Institute of Standards and Technology and any parties acting on its behalf, a royalty-free, non-exclusive, irrevocable, worldwide license to display publicly and use for promotional purposes the contestant's entry ("demonstration license"). This demonstration license includes posting or linking to the contestant's entry on the Department of Commerce, National Institute of Standards and Technology websites, including the challenge website and inclusion of the contestant's submission in any other media, worldwide.
- Any data generated in the evaluation of contestant submissions is the property of the Department of Commerce, National Institute of Standards and Technology. The contestants, reviewers, and judges involved in the evaluation acknowledge and agree that NIST will own this evaluation data, and that the evaluation data created can be used in future research and development activities. To the extent that NIST is able to, NIST will anonymize for research purposes, whether it is used internally or published, any such data and will not include any contestant's, reviewer's, or judge's personally identifiable information. The contestant acknowledges and agrees that the data generated through evaluation of submissions may be used by NIST for future research related to the challenge.

Warranties

Each contestant represents and warrants that the contestant is the sole author and copyright owner of the submission; that the submission is an original work of the contestant; and that the contestant has acquired sufficient rights to use and to authorize others, including the Department of Commerce, National Institute of Standards and Technology, to use the submission, as specified throughout the Official Rules, that the submission does not infringe upon any copyright or upon any other third party rights of which the contestant is aware; and that the submission is free of malware.

The contestant represents and warrants that all information submitted is true and complete to the best of the contestant's knowledge, that the contestant has the right and authority to submit the entry on the contestant's own behalf or on behalf of the persons and entities that the contestant specifies within the entry, and that the entry (both the information and materials submitted in the

entry and the underlying technology/method/idea/treatment protocol/solution described in the entry):

- is the contestant's own original work, or is submitted by permission with full and proper credit given within the entry;
- does not contain proprietary or confidential information or trade secrets (the contestant's or anyone else's);
- does not knowingly violate or infringe upon the patent rights, industrial design rights, copyrights, trademarks, rights in technical data, rights of privacy, publicity or other intellectual property or other rights of any person or entity;
- does not contain malicious code, such as viruses, malware, timebombs, cancelbots, worms, Trojan horses or other potentially harmful programs or other material or information;
- does not and will not violate any applicable law, statute, ordinance, rule or regulation, including, without limitation, United States export laws and regulations, including but not limited to, the International Traffic in Arms Regulations and the Department of Commerce Export Regulations; and
- does not trigger any reporting or royalty or other obligation to any third party.

No Confidential Information

Each contestant agrees and warrants that no part of its submission includes any trade secret information, ideas or products, including but not limited to information, ideas or products within the scope of the Trade Secrets Act, 18 U.S.C. § 1905. All submissions to this prize challenge are deemed non-proprietary. Since NIST will not accept or hold any submitted materials "in confidence" it is agreed that, with respect to the contestant's entry, no confidential or fiduciary relationship or obligation of secrecy is established between NIST and the contestant, the contestant's team, or the company or institution the contestant represents when submitting an entry, or any other person or entity associated with any part of the contestant's entry.

Additional Terms and Conditions

This document outlines the Official Rules for the mFIT Challenge. Nothing within this document or in any documents supporting the mFIT Challenge shall be construed as obligating the Department of Commerce, NIST or any other Federal agency or instrumentality to any expenditure of appropriated funds, or any obligation or expenditure of funds in excess of or in advance of available appropriations.

Challenge Subject to Applicable Law

All challenge phases are subject to all applicable federal laws and regulations. Participation constitutes each contestant's full and unconditional agreement to these Official Rules and administrative decisions, which are final and binding in all matters related to the challenge. Eligibility for a prize award is contingent upon fulfilling all requirements set forth herein. This

notice is not an obligation of funds; the final award of prizes is contingent upon the availability of appropriations.

Participation is subject to all U.S. federal, state and local laws and regulations. Contestants are responsible for checking applicable laws and regulations in their jurisdiction(s) before participating in the prize challenge to ensure that their participation is legal. The Department of Commerce, National Institute of Standards and Technology shall not, by virtue of conducting this prize challenge, be responsible for compliance by contestants in the prize challenge with Federal Law including licensing, export control, and nonproliferation laws, and related regulations. Individuals entering on behalf of or representing a company, institution or other legal entity are responsible for confirming that their entry does not violate any policies of that company, institution or legal entity.

Resolution of Disputes

The Department of Commerce, National Institute of Standards and Technology is solely responsible for administrative decisions, which are final and binding in all matters related to the challenge.

In the event of a dispute as to any registration, the authorized account holder of the email address used to register will be deemed to be the contestant. The "authorized account holder" is the natural person or legal entity assigned an email address by an Internet access provider, online service provider or other organization responsible for assigning email addresses for the domain associated with the submitted address. Contestants and potential winners may be required to show proof of being the authorized account holder.

Publicity

The winners of these prizes (collectively, "Winners") will be featured on the Department of Commerce, National Institute of Standards and Technology website, newsletters, social media, and other outreach materials.

Except where prohibited, participation in the challenge constitutes each winner's consent to the Department of Commerce, National Institute of Standards and Technology's, its agents', and any challenge co-sponsors' use of each winner's name, likeness, photograph, voice, opinions, and/or hometown and state information for promotional purposes through any form of media, worldwide, without further permission, payment or consideration.

Payments

The prize challenge winners will be paid prizes directly from the Department of Commerce, National Institute of Standards and Technology. Prior to payment, winners will be required to verify eligibility. The verification process with the agency includes providing the full legal name, tax identification number or social security number, routing number and banking account to which the prize money can be deposited directly.

All cash prizes to contestants by the Department of Commerce, National Institute of Standards and Technology are subject to tax liabilities, and no withholding will be assessed by the Department of Commerce, National Institute of Standards and Technology on behalf of the contestant claiming a cash prize.

Liability and Insurance

Any and all information provided by or obtained from the Federal Government is without any warranty or representation whatsoever, including but not limited to its suitability for any particular purpose. Upon registration, all contestants agree to assume and, thereby, have assumed any and all risks of injury or loss in connection with or in any way arising from participation in this challenge, development of any application or the use of any application by the contestants or any third-party. Upon registration, except in the case of willful misconduct, all contestants agree to and, thereby, do waive and release any and all claims or causes of action against the Federal Government and its officers, employees and agents for any and all injury, death, damage, or loss of property, revenue, or profits of any nature whatsoever (whether existing or thereafter arising, whether direct, indirect, or consequential and whether foreseeable or not), arising from their participation in the challenge, whether the claim or cause of action arises under contract, tort, or loss through negligence or otherwise. Upon registration, all contestants agree to and, thereby, shall indemnify and hold harmless the Federal Government and its officers, employees and agents for any and all injury, death, and damage of any nature and against third party claims for damages arising from or related to Challenge activities.

Contestants are not required to obtain liability insurance for the mFIT Challenge.

Records Retention and FOIA

All materials submitted to the Department of Commerce, National Institute of Standards and Technology as part of a submission become official records and cannot be returned. Any confidential commercial information contained in a submission should be designated at the time of submission. Submitters will be notified of any Freedom of Information Act requests for their submissions in accordance with 29 C.F.R. § 70.26.

Privacy Advisory

The mFIT Challenge website is hosted by a private entity, Sensis, and is not a service of NIST. The solicitation and collection of your personal or individually identifiable information is subject to the host's privacy and security policies and will not be shared with NIST unless you win the challenge. Challenge winners' personally identifiable information must be made available to NIST in order to collect an award.

508 Compliance

Contestants should keep in mind that the Department of Commerce, National Institute of Standards and Technology considers universal access to information a priority for all individuals, including individuals with disabilities. The Department is strongly committed to meeting its

compliance obligations under Section 508 of the Rehabilitation Act of 1973, as amended, to ensure the accessibility of its programs and activities to individuals with disabilities. This obligation includes acquiring accessible electronic and information technology. When evaluating submissions for this challenge, the extent to which a submission complies with the requirements for accessible technology required by Section 508 will be considered.

General Conditions

All challenge and prize competitions shall be performed in accordance with the America COMPETES Act.

The Department of Commerce, National Institute of Standards and Technology reserves the right to cancel, suspend, and/or modify the challenge, or any part of it, if any fraud, technical failures, or any other factor beyond the Department of Commerce, National Institute of Standards and Technology's reasonable control impairs the integrity or proper functioning of the challenge, as determined by the Department of Commerce, National Institute of Standards and Technology in its sole discretion. The Department of Commerce, National Institute of Standards and Technology is not responsible for, nor is it required to count, incomplete, late, misdirected, damaged, unlawful, or illicit votes, including those secured through payment or achieved through automated means.

NIST reserves the right in its sole discretion to extend or modify the dates of the challenge, and to change the terms set forth herein governing any phases taking place after the effective date of any such change. You agree to the terms set forth herein and to all decisions of NIST and/or all of their respective agents, which are final and binding in all respects.

ALL DECISIONS BY the Department of Commerce, National Institute of Standards and Technology ARE FINAL AND BINDING IN ALL MATTERS RELATED TO THE CHALLENGE.

Appendix A: References and Resources

References

- [1] *Certified Products List*. FBI Biometric Specifications. (2021, June 28).
<https://www.fbibiospecs.cjis.gov/certifications>
- [2] Majumder, S., & Deen, M. J. (2019, May 9). *Smartphone Sensors for Health Monitoring and Diagnosis*. PubMed Central. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6539461/>
- [3] *Electric Biometric Transmission Specification*. FBI Biometric Specifications.
<https://www.fbibiospecs.cjis.gov/EBTS/Approved>

Additional Resources

- Libert, J.M., Grantham, J.D., Bandini, B., Ko, K., Orandi, S., Watson, C. (May 2020)
Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture. NIST Pubs. <https://doi.org/10.6028/NIST.IR.8307>
- Orandi, S., Libert, J.M., Bandini, B., Ko, K., Grantham, J.D., Watson, C. (September 2020)
Evaluating the Operational Impact of Contactless Fingerprint Imagery on Matcher Performance. NIST Pubs. <https://doi.org/10.6028/NIST.IR.8315>
- Orandi, S., Watson, C., Libert, J.M., Fiumara, G.P., Grantham, J.D. (March 2021) *Contactless Fingerprint Capture and Data Interchange Best Practice Recommendation*. NIST Pubs. <https://doi.org/10.6028/NIST.SP.500-334>