the Official Rules document:
Expanding the SIM Card Use for Public Safety Challenge

Challenge Host:

The National Institute of Standards and Technology's
Public Safety Communications Research Division

April 2019 – October 2019

Table of Contents

INTRODUCTION

Overview:
The National Institute of Standards and Technology (NIST)'s Public Safety Communications Research (PSCR) Division and its co-sponsors are requesting solvers' assistance to explore the possibilities for using the Universal Integrated Circuit Card (UICC), commonly known as the SIM card, as a secure storage container for public safety application credentials. Solvers are encouraged to participate in the *Expanding the SIM Card Use for Public Safety Challenge* (the "Challenge") for a total prize purse of up to $100,000.

Challenge Background:
Public Safety personnel utilize their mobile devices to access sensitive information during every day job requirements and emergency situations. For improved communications, public safety needs a secure mechanism for storing sensitive information; current external secure storage solutions can be bulky and cumbersome to use in emergency situations and can be expensive for public safety units with limited budgets to acquire and manage. Also, current standards to access secure applications or information encourage two-factor authentication, often requiring the use of extra hardware, such as a token or a smart card, which inflates costs and increases time in an emergency.

PSCR and their co-sponsors are requesting solvers' assistance to explore the possibilities for using the Universal Integrated Circuit Card (UICC), commonly known as the SIM card, as a secure storage container for application credentials. The SIM card, already used in every mobile device, has characteristics that make it a robust storage device for critical mobile network subscriber data. The SIM card is a tamper-resistant hardware storage container and, if utilized as an application credential storage container, would enable applications to use the authentication credentials provisioned to it seamlessly. The SIM card offers several usability benefits for public safety, as it would be more user friendly; allow networks to provision credentials over-the-air via a secure channel; and potentially enable device sharing by keeping sensitive information on the removable SIM card. Additionally, as the SIM card is currently used in every mobile device, it could offer cost savings for public safety units as extra hardware would not be necessary.

Since 2002, PSCR has collaborated with first responders, stakeholders, and innovators to ensure the development of reliable, intuitive, and mission-focused technologies for the public safety community. PSCR recognizes how cybersecurity affects every aspect of public safety communication. PSCR serves to develop and enhance security solutions to current and future public safety communications. This current Challenge complements public safety-specific Federated Identity Credential and Access Management (ICAM) research conducted by PSCR with other NIST laboratories, such as NIST's Information Technology Laboratory and their National Cybersecurity Center of Excellence.

Challenge Goals and Objectives:
The purpose of this Challenge is to assess the potential of using the SIM card as a secure storage container for public safety application credentials. The Challenge consists of three phases which require contestants to demonstrate that the SIM card can be utilized as a secure storage container as well as develop a mobile application that utilizes a credential, provisioned to the SIM card, to authenticate to third-party service provider(s). This Challenge also seeks to convene first responders, mobile device providers, network providers, authentication providers, researchers, and innovators in order to collaborate and advance the state of mobile device security for public safety.

Should a contestant prove successful, their solution could provide significant time and cost savings for public safety units; for example, the solution would provide:

- Increased security of public safety data on mobile/portable devices;
- Additional credential storage container without an external, bulky device;
- Sharing of mobile devices by multiple users by exchanging SIMs;
- Spur ideas for other potential hardware authentication solutions on mobile devices;
- Increased versatility by adding the ability to provision credentials to the SIM card remotely; and
- Potential cost savings as public safety units would not need to purchase separate hardware authentication tokens.

PSCR will award up to $100,000 to the winners of the Challenge. After the completion of this Challenge, PSCR will keep the submitted prototypes for future public safety demonstrations.

A summary of the phases, the timeline and the Official Rules for the *Expanding the SIM Card Use for Public Safety Challenge* follows:

Phases	Contest Description	Review Criteria Summary	Number of Contestants Eligible to Compete	Awards
1	Concept Paper	Best approach, strongest concept, feasibility, and write up.	Open to all eligible contestants	Up to 20 contestants will be awarded an invitation to participate in Phase 2, Challenge Kickoff Webinar and awarded $1,000.
2	Proof of File Stored on SIM Card	Detailed methodology write-up and a webinar and screen share session	Up to 20 contestants	Up to 10 contestants will be awarded an invitation to participate in Phase 3 and $2,000.
3	Mobile Application and Authentication	Contestants will receive points for verified authentication with FIDO2 service providers. Contestants will send the device to PSCR for evaluation of application.	Up to 10 contestants	Up to 5 final awards: 1st: $30,000; 2nd: $15,000; 3rd: $7,500; Creativity in Public Safety Award (optional): $4,000; and Most Commercially Promising Award (optional): of business technical assistance valued up to $3,500.

Program Email Address

Questions about the Challenge should be directed to psprizes@nist.gov.

Summary of Important Dates (all in 2019)

Phase	Contestant Start Date	Contestant's Submission Due Date	Demo	Judge and Notification of Phase Results Due Date
Phase 1 – Concept Paper	April 3	May 15	N/A	June 3
Phase 2 - Proof of File Stored on SIM Card	June 3*	July 26	July 29 - August 2	August 14
Phase 3 - Mobile Application and Authentication	August 14	October 9	N/A	October 23

NIST reserves the right to revise the dates.
* PSCR anticipates hosting the Challenge Kickoff Webinar on June 4th. Contestants who submit a concept paper will receive a tentative notice with the time and date of the Challenge Kickoff Webinar. However, only successful candidates from Phase 1 will be invited to the Challenge Kickoff Webinar.

Official Rules

SUMMARY OF CHALLENGE

This Challenge consists of three integrated phases that range from concept design to the final phase, where contestants create a mobile application that utilizes a credential stored on the SIM card that can complete authentication, verified by FIDO2 service providers. Each contestant will be evaluated individually against the listed evaluation criteria, and successful contestants will be invited to move to the next phase. Invited contestants will be awarded cash prizes at the end of Phase 1 ($1,000) and Phase 2 ($2,000) to assist with developing a prototype for Phase 3. The scores from the final phase will be the basis for the final prize challenge awards. In addition to cash prize awards, contestants will be given the opportunity to obtain feedback from industry, such as the co-sponsoring entities, through planned webinars and other sessions, in an effort to advance both their prototypes and their connections in the public safety and communications technology communities.

The following is a summary of the various roles and definitions of the contestants and other Challenge participants:

Contestant: an individual, team or a group of teams who submit a solution to the Challenge. Please see the complete eligibility requirements for contestants under the Terms and Condition section of the Official Rules.

Official Representative: the designated point of contact for each contestant. The Official Representative (individual or team lead, in the case of a group project) must be age 18 or older and a U.S. citizen or permanent resident of the United States or its territories. That designated individual will be responsible for meeting all entry and evaluation requirements. NIST will award the prizes in a single dollar amount to the Official Representative. The Official Representative is solely responsible for allocating any prize amount among its member contestants as they deem appropriate.

FIDO2 service provider(s): this entity (entities) collaborates with PSCR as co-sponsors of this Challenge. The service provider(s) participate in the FIDO Alliance, a group that describes itself as an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO2 service provider(s) will provide

contestants with the tools and services required to validate successful implementation of the FIDO2 authentication standard. This will be accomplished by providing all contestants access to authenticate against the FIDO2 service providers' FIDO2 certified server, as well as access to log files and other troubleshooting information, as facilitated by PSCR. At the start of Phase 3, contestants will be invited to a webinar and/or session with the FIDO2 service provider(s) participating in this Challenge. During this session, they will describe more about their role, FIDO Alliance, FIDO2 specifications and how solvers can utilize their services to test and validate FIDO2 authentication. The service provider(s) will, in turn, share with PSCR which contestants successfully completed a FIDO2 based authentication during the Challenge.

Subject matter expert (SME): an expert in their respective field, either from NIST or from a collaborating entity. SMEs will conduct independent reviews of the submissions received from the Challenge. SMEs are not members of the Judging panel and, as such, will provide recommendations based on the evaluation criteria to the Judging panel and will not make any award determinations.

Judging panel: the Director of NIST, Dr. Walter Copan, will select members from the public safety industry, first responders, and PSCR to test and evaluate the submissions for the Challenge. The Judging panel will take SMEs' recommendations into consideration when evaluating contestants' submissions. The Judging panel will make the final determination of awards for the Challenge.

Official Rules of Phase 1: Concept Paper

Introduction:

The Concept Paper 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 securely store and then utilize authentication credentials on the SIM card for first responders. Contestants should include a materials list and/or describe how they will utilize the $1,000 for Phase 2 should they advance to Phase 2: Proof of File Stored on SIM Card. Contestants should also note that the Judging panel will ensure that their plan makes use of existing SIM card standards and FIDO authentication standards. The Judging panel will select up to 20 contestants, invite them to participate in Phase 2 and award $1,000 per contestant for use in developing their prototypes for participation in that phase.

Important Dates:

Concept Paper: Launch on April 3, 2019 with concept papers due May 15, 2019; Contestants will be notified by June 3, 2019 if they were awarded an invitation to Phase 2.

How to Enter:
Visit Challenge.gov, review the series of contests in the Expanding the SIM Card Use for Public Safety Challenge.

- Complete the submission requirements for the Concept Paper Contest; submit the required concept paper as your entry and register as a contestant via Challenge.gov by the required date.
- Submit only one concept paper that reflects your most promising solution.
- Group your entire proposal and contents for the concept paper contest in one PDF document. The size of the attached PDF document must be less than 100MB.

Concept Paper Content Requirements

The concept paper must conform to the following content requirements:

SECTION (Start each section on a new page)	PAGE LIMIT	DESCRIPTION
Cover Page and Abstract (required)	1 page maximum	Include: • Contestant's Name (Team, Organization or Company Name) and list of individual team member(s), • Contestant's Location (City, State/Region and Country). • Contestant's Logo • Official Representative and their preferred contact information. Describe succinctly (500-word MAXIMUM): • The unique aspects of the contestants' approach and the potential impact that the proposed approach could have in achieving the goals of the Challenge. • Note: Do not include proprietary or sensitive information in this summary.
Project Description (required)	4 pages maximum	Addressing the scoring criteria should be your primary objective, therefore, create your concept paper to address the criteria. Below are a few options to consider: • The contestant's knowledge, skills, and capabilities as they relate to the goals of the Challenge. • The contestant's proposed solution for meeting the objectives of the Challenge. • The competitive advantage offered by the contestant's approach or solution.
Informational Schematic/Concept (required)	3 pages maximum	A concept sketch (1-3 pages) in a PDF format.
Proposed Materials List (required)	1 page maximum	A comprehensive materials list and brief description of their proposed use in a PDF format that describes the contestant's planned use of the $1,000 awarded in Phase 2.
Resume/Capability Information for Key Team Members (required)	3 pages maximum	Description of the key team members and why they are well-suited to accomplish the project, with supporting resume and/or capability information to support their qualifications and skills.

NIST makes an independent assessment of each concept paper based on the evaluation criteria. NIST will not review or consider incomplete concept papers. During the review, each SME and member of the Judging panel will review entire concept papers to which they are assigned. The review is not done in sections with different reviewers responsible for different assigned sections, therefore, it is not necessary to repeat information in every part of the concept paper. Contestants must use non-confidential terms in their concept papers. Do not include in the concept paper or otherwise submit information deemed to be proprietary, private, trade secret, or in any way confidential.

Concept Paper Evaluation 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 goals of the Challenge (to assess the potential of the SIM Card as a secure storage container for public safety application credentials; to develop a mobile application that utilizes a credential, provisioned to the SIM card; authenticate to a third-party service provider); the understanding of requirements for interacting with the SIM card to provision information; the discussion of standards-based interfaces for writing to and reading from the SIM card.
- **Technical Outcome**: The extent to which the proposed approach provides a plan for the contestant to successfully complete both Phases 2 and 3 of the Challenge, producing a proof of concept implementation that can drive Public Safety Broadband Network innovation.

Criterion 2: Feasibility & Team (30%)

This criterion involves consideration of the following factors:

- **Team**: The extent to which the capability of the contestant 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 contestants. Reviewers will evaluate: (a) The relevance of the qualifications and experience of the key staff, leadership, and technical experts. (b) The extent of the contestant's prior experience and the quality of the results achieved in leading programs similar in nature to the purpose, scope, etc.
- **Approach**: Contestant's plan to manage the limited schedule, required materials and resources, project risks and other issues, and produce high quality project outcomes, in pursuit of the Challenge goals (to collaborate and advance the state of mobile device security for public safety).

Concept papers will be evaluated based on the criteria above. Each concept paper will be reviewed by at least two SMEs and the Judging panel members and will be assigned a score for each criterion, 0-10 for each criterion. Scores will not be provided to the contestants. In the case of a tie, the Judging panel will decide on the winners invited to compete in Phase 2.

Scoring for Concept Papers

10	Contestant has strong potential to aid in the achievement of the goals of the Challenge
1-9	Varying degrees of certainty the contestant may have the potential to aid in the achievement of the goals of the Challenge
0	Contestant does not have the potential to aid in the achievement of the goals of the Challenge

Weighting of Criteria for Concept Papers

Criterion 1: Strategic Alignment & Technical Outcome	70%
Criterion 2: Feasibility & Team	30%

Official Rules of Phase 2: Proof of File Stored on SIM Card

Introduction:

The up to 20 invited contestants who participated in Phase 1 will submit a detailed description of their methodology, including: the programs they used for writing the file to the SIM; the file structure of the SIM including the file location; access rules on the files; and source code and source code snippets of Java applets (optional). They will then sign up for a recorded video webinar and screen share with SMEs and members of the Judging panel to demonstrate their solution for storage on the SIM card. During the webinar, the contestants will demonstrate the following: the process to provision the file to SIM card; storage of file on SIM card; file structure of SIM card, including file's location. The Judging panel will select up to 10 contestants and invite them to the final phase of the Challenge. These 10 contestants will each be awarded $2,000 for additional prototype development in Phase 3.

Important Dates:

Proof of File Storage on SIM Card: Phase 2 commences June 3, 2019; Challenge Kickoff Webinar June 4, 2019*; Submissions are due by July 26, 2019; Recorded Video Demo will occur between July 29- August 2; Contestants will be notified by August 14, 2019 if they were awarded an invitation to Phase 3.

* PSCR anticipates hosting the Challenge Kickoff Webinar on June 4th. Contestants who submit a concept paper will receive a tentative notice with the time and date of the Challenge Kickoff Webinar. However, only successful candidates from Phase 1 will be invited to the Challenge Kickoff Webinar.

How to Enter:

- Phase 1 awardees will receive an email with the information about Phase 2 of the Challenge, such as how to access the prize challenge platform and how they will sign-up for their webinar and screen share session to showcase their Phase 2 solution.
- Phase 1 awardees in this phase will be required to register for a NIST secure file transfer account. Information on this account and how it works can be accessed here: https://nfiles.nist.gov.
- Phase 1 awardees must submit their detailed methodology description through NIST secure file transfer system by July 26, 2019 at 5pm MT.

Kickoff Webinar Requirements

- Each Phase 1 awardee must have their Official Representative attend the Challenge Kickoff Webinar, currently scheduled on June 4, 2019 (time TBD). Other team members are invited to attend.

Detailed Methodology Description Requirements

The Methodology Description should conform to the following content requirements:

SECTION (Start each section on a new page)	PAGE LIMIT	DESCRIPTION
Cover Page (required)	1 page maximum	Include: • Contestant's Name (Team, Organization or Company Name) and list of individual team member(s), • Contestant's Location (City, State/Region and Country). • Contestant's Logo • Official Representative and their preferred contact information.
Methodology Description (required)	5 pages maximum	Include a narrative description of the methodology used to provision the file to the SIM card in a PDF format. Description must include: ● Workflow diagram; ● Detailed description of workflow for writing file to SIM card; ● Description and names of the tools used for writing file to SIM card; ● Clearly provide the absolute file path for the file provisioned to the SIM card; and ● Whether or not custom code was created.
Source Code (optional)	N/A	Include the source code for the file stored on the SIM card, if custom code was developed. This could be code snippets of a Java applet, custom code for provisioning, etc. This optional section may include the following: ● Brief description of its purpose; ● Well formatted code; and ○ For an example of tools to format code, documentation and style guides, please see: ○ Google Coding Extension ○ Google Java Style Guide ○ Python PEP 8
Problems Encountered **(optional)**	2 pages Maximum	If you faced difficulty completing this phase, provide a description in a PDF format to include the following: ● Description of the problems; and ● Attempted solutions and successful solutions.

Requirements of the Demonstration of Solution through Recorded Video Webinar and Screen Share:

During the webinar and screen share session, contestants must demonstrate the following, in collaboration with their previously submitted methodology description, to the SMEs and members of the Judging panel:

- Process to provision the file to SIM card;
- Process to store the file on the SIM card; and
- Navigate through the SIM card file structure to the file's location.

Contestants should also expect a brief question and answer session with the SMEs and members of the Judging panel as part of their webinar and screen share session.

Evaluation Criteria and Judging:

PSCR will initially screen submissions for completeness and compliance with the objectives and Official Rules of this contest. A submission that fails to meet the compliance requirements for the Detailed Methodology Description 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.

Scoring Criteria #1: Detailed Methodology Description (20%)

This criterion involves consideration of the following factors:

- Methodology description;
- Workflow diagram(s) / description(s);
- Tools and programs used for writing file to SIM card;
- File structure of SIM card including file's location; and
- Access rules on file.

Scoring Criteria #2: Demonstration and Screen Share Webinar - Proof of File Stored on SIM Card (80%)

This criterion involves consideration of the following factors:

- Demonstrate the process to provision the file on the SIM card;
- Demonstrate the process to store the file on the SIM card;
- Navigate through the file structure of the SIM card, including file's location; and
- The ability of the contestant to respond to the questions posed by the SMEs and members of the Judging panel.

Official Rules of Phase 3: Mobile Application and Authentication

Introduction:

During the final phase of the Challenge, contestants will utilize their file storage on the SIM card in order to demonstrate how their mobile application A) utilizes a credential stored on the SIM card and B) completes an authentication verified by FIDO2 service provider(s). The contestants will complete a verified authentication withe the FIDO2 service provider(s), and then will send their device for receipt by PSCR by the deadline for final evaluation. The Judging panel will award up to 5 final awards: 1st $30,000; 2nd $15,000 and 3rd $7,500; Creativity in Public Safety Award (optional award by the Judging panel) $4,000 and a Most Commercially Promising Award (optional award by the Judging panel) of business technical assistance services valued up to $3,500.

Important Dates:

Mobile Application and Authentication: Launch on August 14, 2019; Device must be received by PSCR by October 9, 2019; Contestants will be notified of final awards by October 23, 2019

How to Enter:

- Phase 2 awardees will receive an email with information on the objectives and timeframe for Phase 3 activities.
- At the beginning of Phase 3, the FIDO2 service provider(s) will offer a webinar/session to describe their service, provision accounts for the Phase 2 awardees, and review the process for authenticating to their servers; the Official Representative must attend the webinar and additional team members are welcome to attend.
- Phase 2 awardees must develop their solution and successfully authenticate to the FIDO2 service provider(s) using a credential stored on the SIM card.

- Phase 2 awardees must submit their mobile application along with source code, hardware device (e.g., mobile phone, developer board, etc.) with SIM card, and instructions on how to use their solution (e.g., readme file, how to access device).
- Phase 2 awardees must submit the source code and instructions on how to use their solution through NIST Secure File Transfer system for evaluation by the deadline, October 9th. Contestants must ship the device containing the mobile application and SIM card with tracking identification and have it received by PSCR for evaluation by the deadline, October 9th.

Evaluation Criteria and Judging:

PSCR will initially 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.

Scoring Criteria #1: Compliance Testing (Pass/Fail)

The compliance testing includes:

- The device and mobile application can be accessed by SMEs and members of the Judging panel.
- The device and mobile application do not pose a risk to any SMEs or members of the Judging panel, nor the NIST information technology system nor its lab equipment.
- The source code for the mobile application and instructions on application use were submitted.

Scoring Criteria #2: Verified Authentication with FIDO2 Provider(s) (Max 40/100)

The FIDO2 service provider(s) will work with PSCR to verify contestants' successful authentication with the FIDO2 service provider(s)' servers. If multiple FIDO service provider(s) are available for contestants' successful authentication, the eligible points for this section will be divided equitably.

Scoring Criteria #3: Credential & Application Storage on SIM card (Max 50/100)

- The authentication credential is stored on the SIM card.
- The application can access the credential on the SIM card.
- The application clearly shows the location and is able to view the credential including all data elements.

Scoring Criteria #4: User satisfaction of mobile application (Max 10/100)

- The application is intuitive and should not interfere with the participant's primary task.
- The application demonstrates the contestants' knowledge of public safety requirements, missions, operations, and tasks, particularly how a first responder would access and utilize the mobile application.

Terms and Conditions

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.
- No NIST logo - submission(s) must not use NIST's logo or official seal and must not claim NIST endorsement.
- 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.
- 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 containing any matter which, in the sole discretion of NIST, is indecent, defamatory, in obvious 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 award. NIST shall have the right to remove any content from the Event 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.

Judging Panel

The submissions will be judged by a qualified panel of expert(s) selected by the Director of NIST. The panel consists of Department of Commerce, National Institute of Standards and Technology and non-Department of Commerce, National Institute of Standards and Technology experts who will judge the submissions using the judging criteria identified above and will select winners. Judges will not (A) have personal or financial interests in, or be an employee, officer, director, or agent of any entity that is a registered contestant in a contest; or (B) 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 the "Important Dates" section of these rules.

Verification of Potential Winners

ALL POTENTIAL CONTEST 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

Potential winners 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 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.

Eligibility Requirements:

A contestant (whether an individual, team, or legal entity) must have registered to participate and complied with all of the requirements under section 3719 of title 15, United States Code as contained herein. At the time of entry, the Official Representative (individual or team lead, in the case of a group project) must be age 18 or older and a U.S. citizen or permanent resident of the United States or its territories. In the case of a private entity, the business shall be incorporated in and maintain a place of business in the United States or its territories.

Contestants may not be a Federal entity or Federal employee acting within the scope of their employment. NIST Associates are not eligible to enter. Individuals currently receiving PSCR funding through a grant or cooperative agreement are not eligible to apply. Previous and current PSCR prize challenge contestants are eligible to apply. Non-NIST Federal employees acting in their personal capacities should consult with their respective agency ethics officials to determine whether their participation in this

Competition is permissible. A contestant shall not be deemed ineligible because the contestant consulted with Federal employees or used Federal facilities in preparing its submission to the Challenge if the Federal employees and facilities are made available to all contestants on an equitable basis. Employees of any official co-sponsoring entities are not eligible to enter.

Contestants, including individuals and private entities, 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.

Multiple individuals and/or legal entities may collaborate as a group to submit a single entry and a single individual from the group must be designated as an Official Representative for each entry. That designated individual will be responsible for meeting all entry and evaluation requirements.

TEAMS:

Contest submissions can be from an individual, a team or a group of teams who submit a solution to the Challenge. If a team of individuals, a corporation, or an organization is selected as a prize winner, NIST will award a single dollar amount to the Official Representative. The Official Representative is solely responsible for allocating any prize amount among its member contestants as they deem appropriate. NIST will not arbitrate, intervene, advise on, or resolve any matters between entrant members. It will be up to the winning team(s) to reallocate the prize money among its member contestants, if they deem it appropriate.

Submission Rights:

Any applicable intellectual property rights to a submission will remain with the contestant. By participating in the competition, the contestant is not granting any rights in any patents, pending patent applications, or copyrights related to the technology described in the entry. However, by submitting a contest submission, 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 the right to review the submission, to describe the submission in any materials created in connection with this competition, and to screen and evaluate the submission, and to have the Judges, Challenge administrators, and the designees of any of them, review your 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 competition.
- As part of its submission, the contestant must provide written consent granting the Department of Commerce, National Institute of Standards and Technology, 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 competition website and inclusion of the contestant's submission in any other media, worldwide.

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.

By submitting an entry, 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.
- By making a submission to this prize competition, each contestant agrees 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 competition are deemed non-proprietary. Since NIST does not wish to receive 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 *Expanding the SIM Card Use for Public Safety Challenge*. Nothing within this document or in any documents supporting the *Expanding the SIM Card Use for Public Safety 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 contest. 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 competition 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 competition, be responsible for compliance by Contestants in the prize competition 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 contest.

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 competition 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.

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 contest, 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 and damage 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 contest, whether the claim or cause of action arises under contract or tort. 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 and damage of any nature whatsoever (whether existing or thereafter arising, whether direct, indirect, or consequential and whether foreseeable or not), including but not limited to any damage that may result from a virus, malware, etc., to Government computer systems or data, or to the systems or data of end-users of the software and/or application(s) which results, in whole or in part, from the fault, negligence, or wrongful act or omission of the contestants or contestants' officers, employees or agents.

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.

508 Compliance

Contestants should keep in mind that the Department of Commerce, National Institute of Standards and Technology considers universal accessibility to information a priority for all individuals, including individuals with disabilities. In this regard, 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 contest, 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 Reauthorization Act of 2010, Pub. Law 111-358, title I, § 105(a), Jan. 4, 2011, codified at 15 U.S.C. § 3719 and amended by the American Innovation and Competitiveness Act of 2016 (Pub. L. No. 114-329) (hereinafter "America COMPETES Act").

The Department of Commerce, National Institute of Standards and Technology reserves the right to cancel, suspend, and/or modify the contest, 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 contest, 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. By entering, 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 CONTEST.