TECH TO PROTECT CHALLENGE

Program Rules

1. INTRODUCTION

1.1 OVERVIEW

The Tech to Protect Challenge is an open innovation opportunity led by the National Institute of Standards and Technology (NIST), Public Safety Communications Research (PSCR) Division. Taking place throughout 2019 in ten different cities across the country, the challenge features ten contests which allow for on-line and in-person participation. Each contest is designed to develop new, creative technologies to address issues faced by fire, law enforcement and EMS emergency responders.

The Tech to Protect Challenge is designed to engage entrepreneurs, technologists, students, programmers, designers and public safety experts to create solutions across critical technical areas of public safety communications, including secure communications, location-based services, public safety data analytics, mission-critical voice and user interface/user experience (UI/UX). The participant proposed solutions will support emergency responders' use of advanced communications technologies in accomplishing their day to day activities, critical responsibilities in emergencies, and beyond.

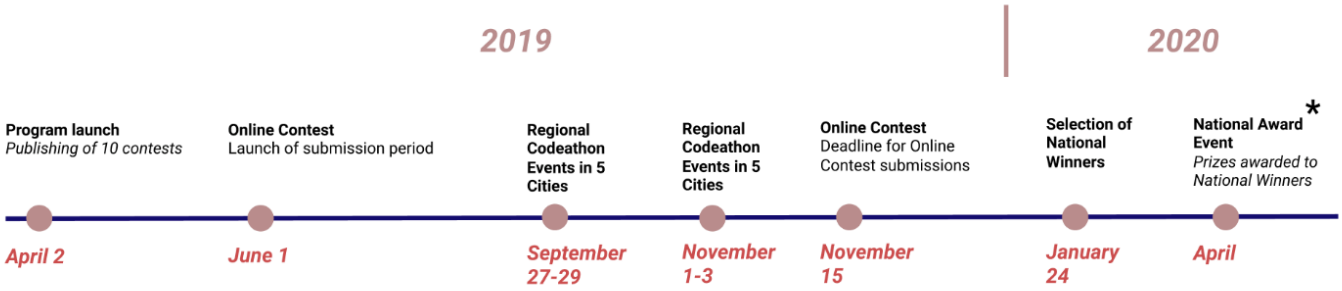
Over the course of 2019-2020, the challenge will include ten unique contests, host ten codeathons in cities across the United States, and award up to $2.2 million in cash prizes to participants. The challenge invites participants of all skill levels; provides opportunities to engage with subject matter experts; and offers access to resources needed to develop viable technology prototypes and solutions. The ten in-person codeathon events will take place in two bursts, September 27-29 and November 1-3, 2019, with the Online Contest launching a rolling application period between June 1 and November 15, 2019. Ultimately, a final national award event will be hosted in April 2020 to showcase and make the final cash awards to the top performing participants.

Participants with diverse skill sets and varying levels of experience are welcome and encouraged to participate:

- Students, professionals and entrepreneurs with technical and non-technical backgrounds including engineers, computer scientists, software developers, designers, communications experts, illustrators, project managers and others.
- Emergency responders and others with an interest in public safety communications with technical and operational experience. This includes individuals with field experience, private and public entities that provide communications products or services, and individuals with an interest in software and hardware elements of communications technologies.

In addition to NIST's Public Safety Communications Research Division, several co-sponsors and partnering organizations will be involved in the implementation of the challenge. The co-sponsors generally include public, private, and civic organizations such as technology solution providers, public safety-focused technology companies, public safety agencies and associations, universities, coding academies, and others — all in support of the participants and the challenge's objectives.

1.2 TIMELINE



* National Winners selected at the National Award Event in April 2020 will continue advancing their projects through the Seed Round Contest and Progress Round Contest between April and October 2020.

1.3 IMPORTANT DATES

Activity	Participants	Awards	Date
Launch of ten public safety communications contests	Open to all eligible participants for early review		April 2, 2019
Online Contest Submission Period Starts Development and online submission of prototypes and solutions by eligible participants	Open to all eligible participants		June 1, 2019
Regional Codeathons burst 1: Development of prototypes and solutions at 5 in-person codeathon events in 5 cities. Up to 4 Local Winners will be selected at each codeathon.	Open to all eligible participants	Up to $35,000 in cash prizes per codeathon event. Anticipated distribution of cash prizes per codeathon: **Local Winners** ● 1st Place $10,000 ● 2nd $7,500 ● 3rd $5,000 ● 4th $2,500 ● Recognition awards — up to ten awards of $1,000 each, one per contest. Local Winners will be showcased on the challenge website.	September 27-29, 2019

Activity	Participants	Awards	Date
Regional Codeathons burst 2: Development of prototypes and solutions at 5 in-person codeathon events in 5 cities. Up to 4 Local Winners will be selected at each codeathon.	Open to all eligible participants	Up to $35,000 in cash prizes per codeathon event. Anticipated distribution of cash prizes per codeathon: **Local Winners** ● 1st Place $10,000 ● 2nd $7,500 ● 3rd $5,000 ● 4th $2,500 ● Recognition awards — up to ten awards of $1,000 each, one per contest. Local Winners will be showcased on the challenge website.	November 1-3, 2019
Online Contest Submission Deadline Submission deadline for the Tech to Protect Online Contest	Open to all eligible participants to enter their best and final submissions for evaluation		November 15, 2019
National Judging Period Starts Judging period starts for national submissions — including submissions to the Online Contest and winning codeathon submissions	Online submissions and final submissions from Regional Codeathons		December 1, 2019
National Judging Period Ends Announcement of National Finalists. National Finalists will be invited to attend the National Award Event.	Online submissions and final submissions from Regional Codeathons	Top performing participants in each of the ten coding contests will be invited as national finalists to participate in the National Award Event.	January 24, 2020

Activity	Participants	Awards	Date
National Award Event Contest Selection and Showcase of National Winners.	Eligible Finalists	Up to $1,850,000 in cash prizes awarded by NIST will be distributed among the National Winners of the challenge. National Winners will be showcased on the challenge website. Up to 30 awards are anticipated for technical excellence in the Demonstration Contest, three in each of the ten unique contests totaling up to $650,000. Up to 12 awards are anticipated in the Seed and Progress Contests totaling up to $1,200,000.	April 2020 April-October 2020

NIST reserves the right to revise the dates.

2. CONTACT INFORMATION

For questions about the Official Rules contact info@techtoprotectchallenge.org or visit www.techtoprotectchallenge.org.

3. HOW TO PARTICIPATE

The Tech to Protect Challenge depends on your participation. We recognize that barriers to entry can be discouraging, so we are committed to making participating the easiest part of the challenge, allowing all of your creative energy to be focused on developing your solution. Here is a step-by-step guide to participation.

1. Visit the Tech to Protect Challenge website (www.techtoprotectchallenge.org). All the information you need to participate is on this site.
2. Participants have **options on how to participate** in the Tech to Protect Challenge:
   a. **Option 1:**

      Register to attend a Regional Codeathon event through the challenge website. Benefits for participants include the opportunity to: compete for cash and in-kind prizes, network and collaborate with other participants to advance public safety, and receive feedback from others on their work. The goal as a participant is to develop and submit a technology prototype or solution addressing one of the challenge's ten unique contests. All completed application materials will need to be submitted before the Regional Codeathon submission deadline through www.techtoprotectchallenge.org. Participants will be required to submit a 3-minute narrated PowerPoint file with a summary of the project, basic information about the team's composition, as well as the specific requirements of the contest that have been addressed. All participant materials will be managed through the challenge website. Participants may attend a Regional Codeathon

event during September 27-29 and/or November 1-3, 2019. Regional Codeathon participants will be encouraged to continue working after the event and submit their "best and final" solutions by November 15, 2019 in the Online Contest.

b. Option 2:

Participate in the Online Contest by developing a prototype or solution that addresses one of the challenge's ten unique contests. Every participant who completes a submission in the Online Contest will be evaluated and eligible for the national prize. All completed application materials will need to be submitted before the Online Contest deadline of November 15, 2019 through www.techtoprotectchallenge.org. Online submissions will require participants to provide a 3-minute narrated PowerPoint file or a 3-minute video describing the submission, general information about themselves, as well as some specific deliverables depending on the contest they are responding to — all participant materials will be managed through the challenge website.

3. Frequently Asked Questions (FAQ) section of the challenge website will provide detailed responses to general issues that are impacting participants and cover the fundamentals of how to interact with the challenge site via text, screen share videos, and other methods to make the website as easy as possible to navigate and use.

4. Continue to engage throughout the challenge by joining our webinars featuring guest speaker emergency responders who use these technologies and can provide context around the use case, and by taking advantage of all the resources the challenge provides to enable your success.

5. Be sure to have your best and final submission submitted by November 15, 2019 — this is the "code freeze" submission deadline for all participants.

4. SUBMISSION PERIOD

1. Regional Codeathon Events

- September 2019 Regional Codeathon Events: In order to be considered for a Regional Codeathon award, participants must meet eligibility requirements, be registered for the Regional Codeathon, attend in person, and must submit their completed materials between September 27-29, 2019.
- November 2019 Regional Codeathon Events: In order to be considered for a Regional Codeathon award, participants must meet eligibility requirements, be registered for the Regional Codeathon, attend in person, and must submit their completed materials between November 1-3, 2019.

2. Online Contest

In order to be considered for a national prize, participants must meet eligibility requirements, and must submit their completed materials at any point between June 1, 2019 at 12:00 PM Eastern Daylight Time (EDT / UTC-4) and November 15, 2019 at 5:00 PM Eastern Standard Time (EST / UTC-5).

3. National Award Event Contest

Top participants from the Online Contest will be invited to participate in the final phase of this challenge. Invitations to the National Award Event Contest are anticipated to be delivered in January 2020, with the National Award Event hosted in April 2020.

5. CONTEST EVALUATION PROCESS

5.1 PERIODS OF EVALUATION

Activity/Period	Description	Objectives	Judge Panel
Codeathon burst 1 Period 1	Evaluation of submissions from 5 Regional Codeathon events on September 27-29, 2019.	Selection of up to the top 4 Local Winners at each codeathon event. Selection of up to ten submissions per event, to recognize one per unique contest.	Panel 1
Codeathon burst 2 Period 2	Evaluation of submissions from 5 Regional Codeathon events on November 1-3, 2019.	Selection of up to the top 4 Local Winners at across each codeathon event. Selection of up to ten submissions per event, to recognize one per unique contest.	
Online Contest Period 3	Evaluation of consolidated submissions, including online submissions and final submission from Regional Codeathons.	Selection of up to the top 20 participants in each of the ten unique contests, to complete final testing and assessment. Following final testing and assessment, selection of up to the top 5 National Finalists in each of the ten unique contests to be invited to the National Award Event.	Panel 2
National Award Event Contest Period 4	Evaluation of National Finalists for the selection of National Winners.	Selection of National Winners for each of the ten unique contests in the Demonstration Contest, as well as the Seed and Progress Contests.	Panel 3
National Award Event Contest Period 5	Evaluation of Seed Contest Winners	Selection of Progress Contests Winners.	Panel 4

5.2 JUDGING PANELS

Three judging panels will operate in a chronological series. Panels will be composed of a diverse group of individuals with specialized skills and experience relevant to the evaluation periods' objectives. Each individual judge is appointed by the NIST Director, and required to sign a non-disclosure agreement (NDA) and conflict of interest (COI) disclosure to ensure that all participant materials are held in confidence and all judging is fair for participants.

The Judge panel consists of experts who will evaluate the participants' submissions according to the criteria defined for each contest. The objective of the judging will be to rank and select the top submissions in each period of evaluation. The decisions of the judges for the contest will be announced in accordance with the dates noted in the "Important Dates" section of these rules.

In support of the judges and the evaluation process, reviewers are subject matter experts covered by NDA and COI requirements, who focus on implementing specific elements of the evaluation process. Reviewers provide evaluation support by assisting with the facilitation of the contests, implementing test and assessment activities, and other processes that generate data for the consideration of the judges, who are responsible for considering all the information and making the final decisions.

Panel 1: Regional Codeathon Judging Panel
The Regional Codeathon Judging Panel will be established to support the evaluation of submissions at each Regional Codeathon event. The judges will coordinate between individual codeathon events, in burst 1 and burst 2, to ensure consistency and uniform implementation of evaluation process.

Panel 2: Online Contest Judging Panel
The Online Contest Judging Panel will be established to support the consolidated evaluation of online submissions and the "best and final" updated versions of Regional Codeathon submissions. The consolidated evaluation will be completed between November 15, 2019 and January 27, 2020 through an online judging process.

Panel 3: National Award Event Contest Judging Panel
The National Judging Panel will be established to select the National Winners of the Tech to Protect Challenge. The final evaluation will be completed in-person at the National Award Event in April 2020.

Panel 4: National Award Event Contest Judging Panel
Following the completion of the Seed Contest, this Judging Panel will convene to evaluate the final submissions from Seed Contest Winners, and determine the Progress Contests Winners.

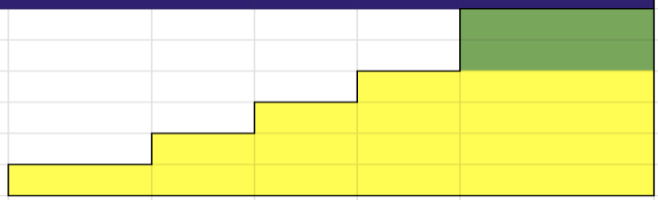
5.3 EVALUATION CRITERIA

What determines the winners? This challenge includes ten unique contests and the evaluation process is designed to be as straightforward and simple as possible for participants to navigate. The graphic below represents the evaluation process that will be applied universally across all contests.

Each contest includes evaluation criteria 0-5. Criteria 0 is a basic pass/fail compliance checklist of minimum requirements for submissions. Beyond the minimum requirements check, contests include up to five technical criteria used to evaluate submissions. Each technical criterion is weighted at 10-40 points out of a total of 100 points. Criteria items 0 through 3 will be used to evaluate Regional Codeathon and Online Contest submissions. Criteria items 4 and 5 represent the most advanced criteria items and will be used to evaluate the top submissions from the Online Contest, prior to selecting the National Finalists. Each of these five criteria items represent different features and attributes that the participant submissions

will need to clearly demonstrate to the judges. The same evaluation process will be used throughout the challenge, with variation by contest for criteria 4-5. Each contest area has unique criteria, but in general examples may include aspects such as the application's UI/UX operability, accuracy, effectiveness, relevance to the contest's sample use case, and other similar elements.

Technical Criteria #	Eval Rating
5	20/100
4	20/100
3	20/100
2	20/100
1	20/100
0	Pass/Fail



5.4 REGIONAL CODEATHON EVALUATION

Objectives:

- Selection of up to the top 4 submissions per Regional Codeathon event.
- Selection of one submission per contest (up to ten total) to be recognized at each Regional Codeathon event.

Process:

Regional Codeathon submissions will be evaluated by judges and reviewers at the end of each 48-hour codeathon event. **Codeathon submissions will be evaluated against criteria items 0 through 3** for a total of 60 rating points out of 100. A specific judging approach will be followed at the codeathon event, as described below. Participants will not be provided oral or written feedback based on the evaluation of their submissions.

Judging Phases	Evaluation Process
Phase 1 **Initial compliance check** Criteria #0 **Objective:** Initial assessment on evaluation criteria #0 items	• During the last day of each codeathon event, before the code freeze submission deadline, judges will review the progress of the teams towards meeting the criteria requirements of each respective contest. Judges will complete this initial review by interacting with participants. Judges will ask two questions to each participant. Judges will take notes on the progress of each participant at this stage during this initial assessment.
Phase 2 **Rapid voting at code freeze** Criteria #0-3 **Objective:** 3-minute review of each project's capabilities and selection of 4 projects or more to proceed to the next phase of evaluation.	• Quick, live demonstrations by the participating teams will be held in person at each participant's station during the rapid voting phase of each Regional Codeathon event. These demonstrations should happen right after the coding freeze deadline and last no longer than 3

	minutes each. Participant teams should showcase the capabilities of the solutions and prototypes developed during this phase. SMEs and judges will rotate station to station to review the project demonstrations by the various teams. ● SME reviewers and judges will evaluate participant submissions by inputting a simple yes or no for each project in a form provided by the national organizers. These votes should be an approximate reflection of whether the teams have met the criteria items 0 to 3, as described in each of the unique contests. ● These ratings will be utilized to narrow down the list of teams that present projects during the next phase.
Phase 3 **Judging Part A** **Participant presentations and judging** Criteria #0-3 **Objective:** Teams present their projects in front of judges and are evaluated based on criteria items 0 to 3 per unique contest.	● Based on the initial voting, judges will invite teams to present their projects through a live presentation and PowerPoint slides. The presentations should take no more than 3 minutes, with an additional 3 minutes being available for questions and answers by the judges. ● Judges will evaluate participant submissions based on criteria items 0 to 3. This evaluation is unique to each contest and may require interactions in addition to the presentation to confirm technical or other elements of the participant's submission. ● Reviewers and judges will evaluate the participant's submission by inputting ratings in a form provided by the national organizers.
Phase 4 **Judging Part B** **Desk review of the submissions and final judging** Criteria #0-3 **Objective:** Detailed desk review of the submissions by the judges. This review will be done remotely, not at the codeathon event.	● Reviewers and judges will be assigned a set of submissions to evaluate. They will evaluate the submission materials and rank them based on criteria items 0 to 3 of the respective unique contest. ● Reviewers and judges will have 2 days after the Regional Codeathon event to submit their rankings. ● Regional Codeathon winners will be formally announced one week after each respective codeathon event.

5.5 ONLINE CONTEST EVALUATION

Objective:

- **Phase 1:** Selection of up to the top 20 submissions from each of the challenge's ten unique contests.
- **Phase 2:** Selection of up to the top 5 finalists from each of the challenge's ten unique contests.

Process:

The Online Contest submissions, which include the "best and final" versions of Regional Codeathon submissions (the online contest only submissions and the "best and final" versions of Regional Codeathon submissions when combined are referred to as "best and final submissions"), will be evaluated to select the challenge finalists through the Online Contest evaluation. Phase 1 of the review will select up to the top 20 submissions for each contest. Phase 2 will evaluate these submissions against criteria items 4 and 5. This evaluation will be done between November 15, 2019 and January 24, 2020 through an online judging process. Up to the top 5 submissions for each contest will be invited to participate in the National Award Event and compete for the final prize awards in April 2020. Participants will not be provided oral or written feedback based on the evaluation of their submissions.

Judging Phases	Evaluation Process
Phase 1 **Desk review of the best and final submissions and judging** Criteria #0-3 **Objective:** Desk review of the best and final submissions based on criteria items 0 to 3 per unique contest.	• Judges will be assigned a set of submissions for online evaluation through the program's submission management and evaluation platform. • Judges will evaluate the participant submissions (application form, video file and any attachments and deliverables required) with the specific criteria 0-3 for the contest. • Judges will evaluate the submissions by inputting ratings in a form within the challenge's submission management and evaluation platform. • The judging process may be assisted by reviewers to implement specific tests, assessments, or other procedures.
Phase 2 **Desk review of the submissions, testing, and final judging** Criteria #4-5 **Objective:** Desk review, testing, and technical assessment of the best and final submissions based on criteria items 4 to 5 per unique contest.	• Reviewers will perform an extensive technical assessment and testing of each participant submission selected in phase 1, as defined in evaluation criteria items 4-5 depending on the requirements for each specific contest. • The results of the technical assessment and testing will be used by the judges in making their selections of the National Finalists of each contest.

5.6 NATIONAL AWARDS EVENT EVALUATION

Participants selected in the Online Contest will be invited to the National Awards Event. Participants will prepare for a live pitch session as part of a NIST managed public event, Demonstration (Demo) Day, to showcase their solution, market entry and scale-up strategy, and a 6-month growth plan. During Demo Day, participants will be evaluated by judges appointed by NIST and in accordance with the evaluation criteria specific to this contest.

6. VERIFICATION OF WINNERS

ALL 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.

Participants must comply with all terms and conditions of the Official Rules. Winning a prize is contingent upon fulfilling all requirements contained herein. The Participants will be notified by email, telephone, or mail after the date of winning results. Each 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) days of the date the notice is sent, an ACH Vendor/Miscellaneous Enrollment Form (OMB NO. 1510-0056) and a Participant 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 Participant 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 of a disqualification of a winner, the Department of Commerce, National Institute of Standards and Technology in their sole discretion may award the applicable prize to an alternate winner, when applicable.

7. SUBMISSION AND ELIGIBILITY REQUIREMENTS

7.1 SUBMISSION REQUIREMENTS

In order for submissions to be eligible for review, recognition and award, Participants 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 address one of the ten contests that are part of the Tech to Protect Challenge.
- Each submission must be the original work of the Participant. The Participant must not knowingly infringe, misappropriate, or otherwise violate any intellectual property rights, privacy rights, or any other rights of any person or entity in the performance of the work.
- It is an express condition of submission and eligibility that each Participant warrants and represents that the Participant's submission is solely owned by the Participant, that the submission is wholly original with the Participant, and that no other party has any ownership rights or ownership interest in the submission. The Participant must disclose if they are subject to any obligation to assign intellectual property rights to parties other than the contest Participant, if the

Participant is licensing or, through any other legal instrument, utilizing intellectual property of another party.

- Each Participant 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.
- While a Participant may contract with a third party for technical assistance to create the submission, the documentation should clearly indicate which components of the solution are the result of the Participant's ideas and creativity (the submission) and which components are from third parties (supporting technology). The Participant must also represent that they own all rights to the submission and all supporting technology.
- Each Submission must be in English and must contain a high-level summary of the submission for public disclosure.
- 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.

7.2 PARTICIPANT ELIGIBILITY

To be eligible for the cash prizes, each Participant or team of Participants must include an individual who is age 18 or older at the time of entry and is 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 primary place of business in the United States or its territories. Participants may not be a Federal entity or Federal employee acting within the scope of their employment. NIST Guest Researchers, as well as direct recipients of NIST funding awards through any Center of Excellence established by NIST, are eligible to enter, but are not eligible to receive cash awards. 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 Participant shall not be deemed ineligible because the Participant consulted with Federal employees or used Federal facilities in preparing its entry to the Challenge if the Federal employees and facilities are made available to all Participants on an equitable basis. Participants, 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. Participants 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. A Participant is eligible to submit a single submission to each contest in Regional Codeathon Burst 1, Burst 2, and the best and final for the Online Contest.

7.3 TEAMS

Contest submissions can be from an individual or a team(s). 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 winning team(s) and each team, whether consisting of a single individual or multiple Participants, is solely responsible for allocating any prize amount among its member Participants 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 Participants, if they deem it appropriate. NIST will not accept duplicate or substantially identical submissions from individual Participants, or teams of Participants. If a situation arises in which a Participant knowingly submits a duplicate or substantially identical submission without an explanation of the circumstances to NIST, NIST may reject that submission or both submissions as noncompliant in its sole discretion. If Participants are submitting as a team, they must provide a complete team roster as part of their submission. The team of Participants is eligible to submit a single submission to each contest in Regional Codeathon Burst 1, Burst 2, and the best and final for the Online Contest.

7.4 SUBMISSION RIGHTS

Any applicable intellectual property rights to a submission will remain with the Participant. By participating in the prize challenge, the Participant is not granting any rights in any patents, pending patent applications, or copyrights related to the technology described in the submission. However, by submitting a contest submission, the Participant is granting the Department of Commerce, National Institute of Standards and Technology certain limited rights as set forth herein.

- The Participant grants to the Department of Commerce and to the National Institute of Standards and Technology, the right to review the submission, to publicly describe the submission in any materials created in connection with this competition, and to screen and evaluate the submission, and to have the Judges, the Challenge administrators, and the designees of any of them, review the submission. The Department of Commerce, National Institute of Standards and Technology will also have the right to publicize Participant's name and, as applicable, the names of Participant's team members and/or organization which participated in the submission following the conclusion of the competition.
- The Participant 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 Participant's entry ("demonstration license"). This demonstration license includes posting or linking to the Participant's entry on the website(s) of the Department of Commerce, the National Institute of Standards and Technology and its competition contractor(s), including the competition website and other media worldwide.

7.5 WARRANTIES

By submitting an entry, the Participant represents and warrants that all information submitted is true and complete to the best of the Participant's knowledge, that the Participant has the right and authority to submit the entry on the Participant's own behalf or on behalf of the persons and entities that the Participant 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 Participant's own original work, or is submitted by permission with full and proper credit given within the entry and that the Participant has acquired sufficient rights to use and authorize others, including the Department of Commerce, National Institute of Standards and Technology, to use the submission;
- contains an accurate public summary acceptable for immediate publication worldwide;
- does not disclose trade secrets (the Participant's or anyone else's);

- does not knowingly violate or infringe upon the patent rights, industrial design rights, copyrights, trademarks, 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.

8. ADDITIONAL TERMS AND CONDITIONS

8.1 CONTEST SUBJECT TO APPLICABLE LAW

This prize challenge competition 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 as amended.

All contests are subject to all applicable federal laws and regulations. Participation constitutes each Participant'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. Participants 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 Participants 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.

All cash prize awarded to Participants 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 Participant claiming a cash prize.

8.2 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 Participant. 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. Participants and potential winners may be required to show proof of being the authorized account holder.

8.3 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 contest constitutes each winner's consent to the Department of Commerce, National Institute of Standards and Technology's and its agents' use of each winner's name, likeness, photograph, voice, opinions, public summary, and/or hometown and state information for promotional purposes through any form of media, worldwide, without further permission, payment, or consideration. The public summary will include the project's title, 200-word project summary, and names and titles of the project's team members.

8.4 PRIVACY, DATA OWNERSHIP AND MANAGEMENT OF PARTICIPANT INFORMATION

Participants understand that the challenge website is hosted by a private entity and is not a service of NIST or the Federal Government. The solicitation and collection of personal or individually identifiable information is subject to the host's privacy and security policies. Personally identifiable information collected on this website will be shared with NIST for prize payment purposes only, and only for winners of the challenge.

Participants acknowledge that they have read the challenge website's data privacy, use, security, and retention policies and understand that all data, except that expressly marked for government use, is subject to these policies. Participants agree not to hold NIST or the U.S. Government liable for the protection, use, or retention of any information submitted through this website.

8.5 LIABILITY

Participants SHALL AGREE TO ASSUME ANY AND ALL RISKS AND WAIVE CLAIMS AGAINS THE Federal Government and its related entities, except in the case of willful misconduct, for any injury, death, damage, or loss of property, revenue, or profits, whether direct, indirect or consequential, arising from participation in this prize competition, whether the injury, death, damage or loss arises through negligence or otherwise.

Insurance: Participants are not required to obtain liability insurance for this Competition.

Indemnification: Participants shall agree to indemnify the Federal Government against third party claims for damages arising from or related to Challenge activities.

8.6. TRADE SECRET INFORMATION

By making a submission to this prize competition, the Participant agrees that no part of its submission includes any Trade Secret information, ideas or products. 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 Participant's submission, no confidential or fiduciary relationship or obligation of secrecy is established between NIST or its affiliates and the Participant, the Participant's team, or the company or institution the Participant represents when submitting, or any other person or entity associated with any part of the Participant's submission.

9. CONTESTS

9.1 CONTEST 1: 360-DEGREE VIEW: A MOBILE DASHBOARD FOR YOUR NETWORK SECURITY

1. INTRODUCTION

1.1 Problem Statement

Public Safety personnel and emergency responders utilize sensors, other wearable devices, and modern communication technologies to preserve life and property. Public safety personnel and emergency responders depend on the security of their devices and communications. To improve the secure use and operations of these devices, a common, unified method for displaying and notifying users of key network information and system/security vitals is needed. These vitals include but are not limited to: network status, devices connected to a Personal Area Network (PAN), the security posture of the network, etc. A centralized dashboard displaying the connection (e.g. Cellular, Wi-Fi, VPN Connections, Bluetooth, NFC, GPS) status of a mobile device can provide useful information for the emergency responder and their IT support personnel. While much of this information is available within the disparate settings of devices, it is often difficult to navigate through the user interface to find the location of this information, and the location of the information is different depending on the device. In addition, limited security contextual information is provided to the user. To re-enforce the effectiveness of this dashboard, a non-intrusive notification to alert the emergency responder of the status of a functioning or malfunctioning connection would save time and effort during an incident or event.

This device vitals dashboard is designed to improve emergency responders' confidence in the communication channels required to relay the sensitive information from the field to the organizational units needed to coordinate and perform lifesaving duties.

For secure communication, public safety needs:

1. An effective dashboard that organizes and displays device connections and available security information for those connections.
2. Intuitive navigation to retrieve detailed information, such as Ciphering Indicator.
3. Status of assets connected to the device, displaying the history of the asset's use if the asset has been connected previously.
4. Asset inventory to help perform analysis, determine the threat landscape for a public safety individual and help identifying rogue and potentially malicious assets or non-secure network connections.

USE CASES

Paramedic responding to an emergency:
During a medical emergency response, a paramedic uses an application to collect a patient's information (name, age, gender, etc.), record the patient's vital signs (heart rate, blood pressure, temperature, etc.), and look up medications. In addition, the app forwards the patient information to the hospital to which the patient will be taken. The paramedic, focusing on their duties, does not necessarily have the information technology background to notice irregularities in the functions of the technology to perform these tasks. The data collected by the paramedic could be lifesaving information to the patient, but this information, in the wrong hands, can enable a malicious actor to commit identity theft with the use of the exposed personally identifiable information.

Undercover officer communications:
As part of a covert operation, an undercover officer is using a mobile application on his/her mobile device to provide operational information back to the operation's command center, relaying confidential informant information, video, voice, location, etc., from the officer. The success of the operation, the informant's life, and the officer's life could depend on the confidentiality of this data. Now, imagine if the undercover officer could see a gauge that displayed the security of the PAN and the undercover officer's device knew to hold on to the video or text message until they returned to a more secure operating environment, reducing the risk of compromising the officer, informant, and information.

1.2 Objectives

The objective of this contest is to create an application that will communicate to emergency responders the security posture of their device via a simplified dashboard and automate the use of different applications based on the level of security related to data arriving and data transmitting from the device. Allowing access control to secure applications should be accessible even if the device's security posture is not fully secure. The dashboard should be able to act as an information source with options, and never impede the emergency responders' mission.

The application will communicate to emergency responders:

1. LTE, Bluetooth, NFC status with security information real-time or simulated for demonstration.
2. Connected device inventory/history, to inform the user of recurring and new, never before connected devices to the UE.
3. Ciphering indicator to inform users of their over-the-air cellular connection encryption status.

1.3 Resources

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

- Software Development:
    - Android Software Development Kit (SDK)
    - A report on accessibility of the APIs into connection information within the designated OS or OS Kits to determine feasibility
    - Synthetic data created by PSCR
- Industry security guidance:
    - Background Security Standards (3GPP SA3) information on displaying LTE security status
    - Criteria for determining security rating of Wi-Fi and VPN connections
- Public Safety community guidance:
    - User Requirements for accessibility of data

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements

Rating: Pass/Fail

- Application will communicate security status and information for:
  - LTE: User data confidentiality and integrity
  - Bluetooth: Current and recent connected devices
  - NFC: Current and recent data transmissions
  - Local hardware encryption: On or Off
  - VPN:
    - Current and recent VPN connections
    - Security Data for current connection (TLS 1.2)
  - Wi-Fi connection
    - Current and recent Wi-Fi connections
    - Security Data for current connection (WPA2)
  - GPS: Status
  - Antivirus application status: On or Off
  - MDM Status: Operating status

Criteria #1

Rating: 20/100

- Application's ability to toggle between the different security and connection settings within the dashboard
  - LTE: User data confidentiality and integrity
  - Bluetooth: Current and recent connected devices
  - NFC: Current and recent data transmissions
  - Local hardware encryption: On or Off
  - VPN:
    - Current and recent VPN connections
    - Security Data for current connection (TLS 1.2)
  - Wi-Fi connection
    - Current and recent Wi-Fi connections
    - Security Data for current connection (WPA2)
  - GPS: On/Off
  - Antivirus application status: On or Off
  - MDM Status: Operating

Criteria #2

Rating: 20/100

- Application's ability to respond to and communicate the changing scenarios provided:
  - Does the application dashboard respond to changing variables within the provided scenarios in a timely manner?
    - LTE security status changes
    - VPN status changes
    - Bluetooth changes
    - Time and location warnings/information

Criteria #3: UI/UX Evaluation (Part 1)[1]

Rating: 20/100

Emergency responder and UI/UX SME judging of:

- Learnability: degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.
- Operability: degree to which a product or system has attributes that make it easy to operate and control.

Criteria #4: UI/UX Evaluation (Part 2)[2]

Rating: 40/100

Emergency responder and UI/UX SME judging of:

- Functional completeness: degree to which the set of functions covers all the specified tasks and user objectives.
- Functional correctness: degree to which a product or system provides the correct results with the needed degree of precision.
- Functional appropriateness: degree to which the functions facilitate the accomplishment of specified tasks and objectives.

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
  - A summary of the submission.
  - Basic information about the participant or participant's team.
  - Specific requirements of the contest that are being addressed by the participants.
  - Two to four screenshots of the solutions or prototype.
  - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

[1] https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0

[2] https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0

9.2 CONTEST 2: NO NEED TO REPEAT: DELIVERING MISSION CRITICAL COMMUNICATIONS

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Today's emergency responders have many technologically advanced tools at their disposal. These tools allow them to perform their lifesaving duties more efficiently and safely. The tools range from mapping, presence availability, body sensors, secured communications to unmanned vehicles carrying communication stations. Out of all the ways to communicate in the present day, voice communication is still the predominant way of communication for emergency responders. Currently, approximately 80% of communication for emergency responders is voice communication. Out of that, approximately 80% is group communication (rather than private calls and other options). This will continue to be true in the coming years, as voice will still be very important for mission critical communications.

The wireless telecom industry recognized the need for emergency responders to have access to group communications. In response to this need, they created Mission Critical Push-to-Talk, or MCPTT, in the 3GPP standards (3rd Generation Partnership Project) for the next generation of voice communications for emergency responders. MCPTT, which is the only standardized method for Push-To-Talk, was created for many reasons. One is to provide an interoperable solution that will allow emergency responders to communicate via Push-To-Talk which is agnostic to network access, devices, and its application services. Second is to provide mechanisms to ensure Mission Critical communications on 4G networks beyond the existing best effort non-mission critical approaches. But, the MCPTT ecosystem resulting from the 3GPP definition is very complex. There are still too many proprietary interfaces and layers in a user device, such as a smartphone. To get around this, many non-standard solutions have been developed. However, these solutions are not fully mission critical-capable and they probably would not receive the standardized priority on the network. Plus, they are not interoperable across devices, applications, and networks. In other words, every emergency responder participating in a mission needs to have the same application and software version (and possibly even the same hardware) in order to communicate. In summary, the problem is that there are no MCPTT applications available and it is simply too difficult to create them. At least that was the situation until MCOP.

MCOP, or Mission Critical Open Platform, is an ongoing project to eliminate the barriers that prevent people from creating MCPTT applications. MCOP found ways to create APIs to move past proprietary layers in the Android OS, as well as in most hardware situations. MCOP then developed an SDK which utilizes these APIs, so developers can easily and quickly build a functioning MCPTT application. As the name of MCOP implies, the SDK is open source and readily available for download and use by application developers. In addition, MCOP has created a free and openly available online portal and testbed that aids developers in testing their MCPTT application. A person just needs to schedule time on the testbed.

1.2 OBJECTIVES

The overall aim of this challenge is to increase the availability of MCPTT standard-compatible applications for emergency responders to use. This will be accomplished by exposing people to the MCOP SDK and testbed. Using the tools of MCOP, any individual or team of people can make a functioning MCPTT application. The expected result from participants of this challenge is a fully functioning and fully compliant MCPTT Android application created using the MCOP SDK that allows emergency responders to communicate while their smartphone is on an LTE network.

In this challenge, many participants will only have access to normal everyday smartphones. When equipped with a standards-compliant MCPTT application created with the MCOP SDK, these everyday smartphones can make MCPTT calls in an excellent manner in many different situations. However, emergency responders may not be able to use a basic smartphone while performing their duties during a life-threatening emergency. Making an MCPTT application that can handle emergency situations is highly encouraged for this challenge as a higher-level endeavor, but participants should focus on making an effective application for non-emergency situations as a first step. To aid participants in this area, two non-emergency scenarios or use cases have been defined. MCPTT applications will be judged based on how well they are able to accommodate these use cases:

1) Firefighters — Of the many duties of firefighters, one is to inspect buildings to ensure that they are up to code. For example, a firefighter may inspect a school to make sure there are adequate fire alarms, functioning fire extinguishers, clutter-free emergency exits, etc. For the "Firefighter" scenario, imagine two firefighters inspecting a large school building. The firefighters split up and go down different areas of the school to save time. They need to be able to communicate in a basic MCPTT private call while performing their duties.

2) Law Enforcement — Many large law enforcement forces have their own Land Mobile Radio, or LMR, systems in order to communicate. However, many officers are also turning to smartphones in addition to their LMR radios. In a typical traffic stop situation, an officer is not going to approach the vehicle while looking down at a smartphone. The officer, for safety reasons, needs to stay alert and watch the passengers in the vehicle. However, there are times when group communications via a smartphone would be beneficial. In the "Law Enforcement" scenario, imagine a group of law enforcement officers that have been assigned to perform security for a popular football game. It is hours before the game starts and fans have not started to arrive. The assigned officers need to meet at Gate 1 of the stadium to go over details of their assignment;. however, the meeting time and location have now changed. The officers need to communicate via an MCPTT group call to inform the team of the new meeting location and time.

The defined use cases are simple; participants are encouraged to expand on the use cases as well as add functionality for other more complex use cases. For example, an MCPTT application may include some form of voice-to-text technology. Or, an MCPTT application adds more standard-based functionality such as the ability to upgrade a basic MCPTT call to an emergency MCPTT call. Participants are not required to include added functionality, and there are no requirements for specific functionality above and beyond the two defined use cases of "Firefighters" and "Law Enforcement" from above. However, applications that include added functionality have the possibility to score more points during the judging process.

1.3 RESOURCES

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided “AS IS” and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

For this challenge, participants are required to use the MCOP SDK to create a fully functioning and fully compliant MCPTT Android application that allows emergency responders to communicate while their smartphone is on an LTE network, and for the users of the application to be able to understand all communication. From the MCOP website: “The Mission Critical Open Platform (MCOP) is a collaborative project with the financial assistance award 70NANB17H151 from U.S. Department of Commerce, National Institute of Standards and Technology through the Public Safety Innovation

Acceleration Program (PSIAP). MCOP aims at facing the challenges of the new MCPTT complex ecosystem through the definition, development and validation of a MCPTT UE Open Platform (MCOP) that identifies neat interfaces between the different technologies in the UEs, reduces the integration efforts and removes the entry barriers." The MCOP project comprises the definition and deployment of a technology neutral platform for MCPTT enabled applications for Public Safety in order to reduce the entry barriers and integration efforts due to the heterogeneity and complexity of the MCPTT ecosystem. The MCOP platform includes the so-called MCOP Unified Open Application API (Northbound API), supporting the interface between the MCPTT applications and the MCOP SDK and the Integration API, responsible for providing Southbound interface from the SDK to the OS-dependent low-level capabilities.

For more information about MCOP, how to download the MCOP SDK, and how to use the online testbed, visit:

- https://www.mcopenplatform.org/
- https://www.mcopenplatform.org/mcop_resources/
- https://demo.mcopenplatform.org/gitlist/mcop/MCOP-SDK.git/

Teams with existing tools are welcome to enhance their products as part of the challenge. For example, a creative team with an existing PTT application that isn't fully MCPTT-compliant can have its functionality enhanced with MCPTT compliance with MCOP. Or perhaps a team with existing hardware, such as a fully functional smartphone or a peripheral for a smartphone, can enhance their product with MCOP during this challenge. A team with enhanced security expertise can include additional security functionality to the created MCPTT application. The possibilities are only limited to the imagination of the challenge participants.

For more information about MCPTT in general and other similar emergency responder communications features, visit:
http://www.3gpp.org/news-events/3gpp-news/1875-mc_services

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements
Rating: Pass/Fail

- The application must be able to make a standards-compliant MCPTT group call.[3] (Pass/Fail)
- The application must be able to make a standards-compliant MCPTT private call.[4] (Pass/Fail)

[3] 3GPP TS 24.379:
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2953
[4] 3GPP TS 24.380

Criteria #1
Rating: 20/100

- Effectiveness: Relevance to the defined use cases and the degree to which emergency responders can recognize how the created application is appropriate or not for their needs in the defined use cases
  - Firefighter — how effective is the application in making a basic MCPTT private call while performing a building inspection
  - Law Enforcement — how effective is the application in making a basic MCPTT group call before meeting at a newly designated location

Criteria #2
Rating: 20/100

- Innovative use of application style and screen orientation to support use cases
- Appearance: Degree to which the application utilizes style and screen orientation

Criteria #3[5]
Rating: 20/100

- Overall usability and design:
  - Learnability (degree to which the created application can be used by emergency responders to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.)
  - Operability (degree to which the created application has attributes that make it easy to operate and control.)
  - User error protection and permissions (degree to which the application protects users against making errors or exposing sensitive information.)
  - User interface aesthetics (degree to which a user interface enables pleasing and satisfying interaction for the user.)
  - Accessibility and Ergonomics (degree to which the created application can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use.)

Criteria #4
Rating: 40/100

- Creativity/ Extra functionality (degree that the application adds extra functionality beyond a basic MCPTT application). Participants must list extra functionalities that are implemented and propose how those can be demonstrated. Below is a list of examples of extra functionalities that a participant could possibly consider, but the list is not exhaustive nor is it a list of required extra functionality:
  - Voice to text capability — there are some situations when an emergency responder is not able to talk or to play the incoming audio during an MCPTT call. Example: The emergency responder still needs to be able to understand what is being said by the speaker during an MCPTT call but without the use of audio.
  - Enhancements for use during emergency situations — in some emergency situations, a basic smartphone is not sufficient for MCPTT communications.

[5] From ISO 25010: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0

Example: The emergency responder needs both hands to perform his or her duties, but still needs to communicate during an MCPTT call.

- Adding location capability — in some situations, knowing the location of the emergency responder is important. Example: A dispatcher needs to deploy an EMT to a location inside a park where there is no specific address. The dispatcher must be able to find nearby EMTs.
- Upgrading and downgrading MCPTT calls — in some situations, an emergency responder may want to upgrade a basic MCPTT call to an MCPTT emergency call or an MCPPT imminent peril call. After the situation deescalates, the emergency responder may want to downgrade the call back to a basic MCPTT call. Example: A law enforcement officer is communicating in an MCPTT group call while on patrol, but then witnesses a crime. The officer wants to quickly and easily upgrade the call to accommodate the new situation. After the arrest has been made, the officer wants to downgrade the call back to a basic MCPTT call.
- Creating temporary groups — in some situations, an emergency responder may want to create a temporary MCPTT group or create a group on the fly. Example: 3 types of emergency responders arrive on a scene (fire, law enforcement, EMT) and they want to communicate via an MCPTT group call using a newly formed and/or temporary group. Members of the group need to be added or removed as emergency responders arrive at the scene and leave the scene.
- Public safety users currently use shared devices for their agency mission critical operations where the phone is used on different shifts. There could be some enhanced capability to identify the user who can receive/originate the call based on the authentication that are already available/supported on the device such as bio-metrics (fingerprint or retina) for locking/unlocking and able to invoke the same credentials for opening MCPTT application for ease of use rather than having multiple login/password access to the MCPTTT application.
- The application may leverage the existing smartphone address book/contacts list, call logs and dialer functions for MCPTT call and groups origination.
- The location and presence capability of the MCPTT user can be rendered on map location on the phone contacts list for enhanced usability.
- The option of MCPTT calls that can be recorded locally and able to store on the device — that is not specific to voice but also text, video with playback capability.
- The enhanced option of identification of the user with Talker ID or UserID or alias capability on MCPTT and group call scenarios. This use case is applicable on shared devices scenario where the person who is making MCPTT call can be identified by the agency in combination of device ID (IMEI) and SIM (IMSI).
- Public Safety users can have the option on prioritizing the groups internally on their groups. The MCPTT application should be able to provide enhanced usability on concurrent talk group request to emergency responder.

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
    - A summary of the submission.
    - Basic information about the participant or participant's team.
    - Specific requirements of the contest that are being addressed by the participants.
    - Two to four screenshots of the solutions or prototype.
    - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.3 CONTEST 3: LOOKING UNDER THE HOOD: USING AUGMENTED REALITY TO HELP SAVE TRAPPED PASSENGERS

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Emergency responders (firefighters, EMS crew, etc.) arrive on the scene of a motor vehicle accident involving a car that has rolled off an embankment and has passengers trapped inside. The responders know they will need to use various extrication tools including the "Jaws-of-Life," but before they grab those tools they need to have access to valuable up-to-date information about the vehicle design and construction to find the most efficient and safest way to gain access to the vehicle to rescue the passengers. This critical information includes, but is not limited to, airbag locations, high pressure struts, and where to make safe extrication entry cuts. One wrong cut could lead to the inadvertent deployment of airbags that could cause further injury or even death of a passenger or an emergency responder. This contest is an opportunity for participants to create an innovative Augmented Reality (AR) mobile application that can provide this information in an intuitive, fast, and effective way to enable the extrication process.

There are existing applications and websites that provide emergency responders with diagrams of vehicles; however, these applications have various shortcomings and limitations: they may be cumbersome to locate the correct vehicle make and model, the orientation of the images do not match the pose of the vehicle in the accident, and the 2D images may be difficult to manipulate and sort through. This contest enables participants to address these limitations by using AR to overlay the critical vehicle information on top of a 3D picture/model and/or real-time image capture of the vehicle to help the emergency responder make the correct decisions during the extrication process. In addition to using AR, we anticipate participants will leverage external datasets, for example DMV records, to reliably identify the year, make and model of the vehicle.

1.2 OBJECTIVES

A mobile application which uses the device camera and vehicle year, make and model (entered manually, or read via a License Plate Reader and queried from DMV records or decoded from VIN) to overlay information about the vehicle, including safe extrication points, overlaid on the image. For the contest, the app should be able to process data from an external database; however, interacting with an actual database or creating a vehicle information database is not required. Participants should anticipate some sample datasets to be provided to assist them in their efforts.

The user should have the ability to control the amount and type of information displayed. For example, specific tips about the vehicle entry cut points (if available) or recommended tools to use can be displayed according to user preferences.

We envision the emergency responder walking around the vehicle pointing the device camera at the vehicle and, in real-time, the application delivers the relevant vehicle information overlaid on top of the image. The app should be able to detect the pose of the vehicle whether it be upside-down or on its side. In addition, the app should be able to identify key elements of the vehicle even in the event of massive damage that has caused significant deformities to the vehicle's shape or appearance. Participants should not anticipate training data such as images of wreckages or damaged cars to be provided to assist them in their efforts.

The application should present information in different modes to provide the emergency responder options when real-time images are not feasible to display the necessary information; i.e. low light environments or where damage is too severe to rely on automatic object recognition. In these situations, there are several options that could be employed by the app: a 3D image of the vehicle could be used as the basis for the information overlays, audio instructions can be provided to emergency responders to tell them where they need to start the extrication process and what tools to use, or some other creative approach.

1.3 RESOURCES

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

In this section, the resources provided are designed to be useful to all participants. The references to data sources should be leveraged for this contest as well as a collection of references to SDKs and APIs that could assist in the development of a solution. Included below are some vehicle images and models that can be used; however, training data on vehicles such as images of vehicles damaged as a result of accidents will not be provided.

Tools and SDKs

- Computer Vision Object Detection System (Commercial): Matroid
- Computer Vision System (Open Source): OpenCV
- ARKit (Apple) https://developer.apple.com/arkit/
- ARCore (Google) https://developers.google.com/ar/

Datasets

- National Fire Protection Association, Emergency Response Guides: https://www.nfpa.org/Training-and-Events/By-topic/Alternative-Fuel-Vehicle-Safety-Training/Emergency-Response-Guides
- Car images (for image processing/automatic identification of vehicle) — Stanford University Car Dataset: https://ai.stanford.edu/~jkrause/cars/car_dataset.html
- Simulated DMV database
- Vehicle Manufacturer Vehicle Construction Data

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements

Rating: Pass/Fail

- Is the app capable of identifying the vehicle? (i.e., object detection, or the ability to identify the form, shape, and outlines of the car caught by the device's camera) (Pass/Fail)
- Is the app capable of identifying sides of the vehicle accurately? (Front, back, driver, and passenger sides)? (Pass/Fail)
- Are the virtual objects (shapes and text) merged correctly with the real world? (Position, scale) (Pass/Fail)
- Do the functions support the objectives of vehicle extrication process? (Pass/Fail)
    - The functions in the application must correspond to the vehicle extrication objectives. There should be no unnecessary actions and interaction.
- Are the information and media content appropriate? (Pass/Fail)
    - The information and media content should appropriately assist the emergency responder in successfully completing the vehicle extrication process. The quality of the information used must be in accordance with the context of public safety communication best practices.
- Loading time of virtual objects in the scene must be < 10 seconds (Pass/Fail)
- Application should have the ability to function offline without connection to a data network (Pass/Fail)
- Does the application meet the vehicle extrication contest fundamental objectives? (Pass/Fail)
    - The objective of use and potential of improving the efficiency of the vehicle extrication process must be clearly identifiable for the user.
    - All functions, assistance, and feedback must be comprehensible and should support the vehicle extrication process.

Criteria #1: Accuracy
Rating: 20/100

- Augmented Reality Information Overlay for the user to visualize information:
    - How accurately the app displays the extrication info during use, such as exact location of the entry cut points
    - Are important internal components/structure of the vehicle around the entry points marked clearly (for example using a color-coding scheme)? This would include location of airbags, high pressure components, or high voltage parts in electric vehicles or other hazards

Criteria #2: Efficiency
Rating: 20/100

- How efficient is the application in assisting emergency responders during the extrication process?
- An imbedded frame rate counter will display a frame rate count of 30-60 frames per second, and this feature will be able to toggle on or off to enable ease of use for emergency responders
- Loading time of virtual objects (measured in seconds)
    - Minimum 5 <= t < 10 seconds
    - Medium: 2 seconds <= t < 5 seconds
    - Maximum: t < 2 seconds
- How well can the user use the application freely while walking around the vehicle?
    - The application will be in use during an operational event and will be handled directly by an emergency responder.

Criteria #3: Reliability
Rating: 20/100

- Does the app provide an alternative method for displaying vehicle extrication info, if the live image is not suitable for use (ex: due to extensive damage to the car, or environmental factors such as lighting or weather conditions)?
    - 2D diagram of the vehicle with textual instructions — Minimum
    - 3D/360 interactive diagram of the vehicle — Maximum
- Advanced features:
    - Animated instructions displaying helpful info such as suggested tools to use, angle of the entry point cuts, etc.
    - Voice over instructions

Criteria #4: Overall User Experience
Rating: 40/100

Likert scale styled assessment on the following items.

- How well is the application designed?
    - The visual aspects of the application must be pleasing to the user and effective in communicating information to the user.

- How evident is it that the developer leveraged public safety SMEs during the development process?
    - The application must be based on a user-centered process; the quality of the research methods and their subsequent integration are decisive for the success of the product.

- Is the use sequence in the application intuitive to the user?
    - The goal is to minimize the learning time of the user to effectively use the application. The information presentation, symbols and the use of color must be self-explanatory and contribute to intuitive user guidance that is consistent with user expectations.

- Is the solution universally intuitive and comprehensible?

- A wide range of different users from varied disciplines in public safety and training must be able to securely operate the application in various operational scenarios; errors in use must be severely minimized with a target of completely eliminated.

- What are the users' overall sentiments about the flow of the application?
  - The sum of expectations, behaviors and reactions before, during and after use of the application must be predominantly positive to earn the trust of emergency responders and to encourage adoption.

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
  - A summary of the submission.
  - Basic information about the participant or participant's team.
  - Specific requirements of the contest that are being addressed by the participants.
  - Two to four screenshots of the solutions or prototype.
  - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.4 CONTEST 4: GOT YOU COVERED: MAPPING LTE CAPABILITIES TO SAVE LIVES

1. INTRODUCTION

The objective of this challenge is to add innovative mapping capabilities to the **LTE Coverage Tool** Android application (https://play.google.com/store/apps/details?id=gov.nist.oism.asd.ltecoveragetool). The application, in its current state, uses a commercial Android smartphone (also known as a UE, or User Equipment) to provide an assessment of LTE (Long Term Evolution) network coverage.

1.1 Problem Statement

Emergency responders work every day in environments which present challenges for communications, depending on installed cellular infrastructure which may not cover remote locations, interior/underground settings or areas where resources have been compromised. As public safety agencies increase their reliance on cellular/LTE communication, they have a critical need for evaluating coverage in these diverse environments — a procedure which requires expensive equipment and training beyond the budgets of most agencies or teams. Addressing that problem, the U.S. Department of Homeland Security (DHS) sponsored work in the National Institute of Standards and Technology (NIST), Communications Technology Laboratory, Public Safety Communications Research (PSCR) Division and the National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Sciences (ITS) to develop and use an experimental Android application which demonstrated that measurements from commercial UEs (smartphones) could provide a reliable assessment. NIST PSCR released the experimental application and source code in 2018, and NTIA ITS will publish a technical report on their findings in 2019.

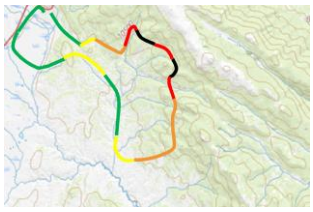
1.2 Objectives

Release of the LTE Coverage Tool application and source code provide agencies with a simple, free tool for making subjective coverage assessments, and a code base for customization or integration with other tools. Other applications are also available at low cost, providing similar capabilities (through proprietary software); some of these can present the data using GPS as an overlay onto a map (e.g., Google Maps or OpenStreetMap); however, no known application provides coverage information with location data for environments lacking GPS coverage. The goal for this challenge is to integrate one or more innovative location mapping elements into the tool which will provide a transformational step forward for emergency responders and will translate directly to saving the lives of emergency responders and citizens. Required output for a successful challenge submission will include a working Android Package (APK file). Applications submitted shall incorporate all functionality from the baseline LTE Coverage Tool with additional capabilities for presenting measurements with associated location data as explained below.

A foundational requirement for the submitted application is that no external equipment may be required. Using only the resources available from a commercial UE, the extended application should support three modes for location tracking and presentation (notional diagrams are presented below). In all modes, the map outputs shall present excellent, good, and poor coverage areas, as determined by the baseline app from Android Reference Signal Received Power (RSRP) measurements.

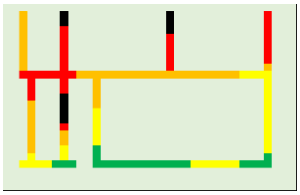
1.2.1 **Mode 1:** Heat map using GPS to present data on a map (primarily for outdoor use).

Mode 1 is intended for the outdoor use case, where an agency may need to assess coverage in advance of an event or in preparation for incidents. GPS coverage is assumed for this case. Mode 1 is the starting point for a submission, since it should be relatively easy to overlay coverage quality data from the baseline app as a heat map.



1.2.2 **Mode 2:** Where no GPS data or building plan is available, represent route as a heat map using internal UE sensors.

For Mode 2, it is assumed that GPS is not available or is intermittent throughout the assessment route. Accessing any internal UE sensors, the application shall generate a conceptual map of a route (walked by a user), such that after completion, the user will be able to discern excellent, good, and poor coverage areas along the route (i.e., within a building).

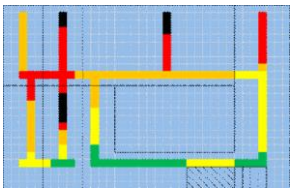


The application shall not access external hardware for position determination or tracking. Innovative mapping presentations are encouraged!

Evaluation routes will include multiple levels, and the application must display levels/floors in some manner (layers, multiple views, 3D view, etc.). Innovation is encouraged!

1.2.3 **Mode 3:** Given a building plan/map and planned route, overlay heat map onto route.

Mode 3 expands upon Mode 2, using the same assumptions and requirements and adding the capability for a user to load a building plan (image file) and plot the conceptual map onto the plan. It is expected that the user would click on the starting point and enter course corrections (corrected locations) along the route. Example image files will be made available to participants.



The primary use case for Mode 3 is intended for site inspections or similar scenarios where an emergency responder would have a building plan prior to starting an assessment.

1.3 Resources

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

- Source code published on the NIST GitHub (required as a base for all submissions): https://github.com/usnistgov/LTECoverageTool
- Template for CSV file which will be required for evaluation.
- Template for building plan (mode 3).

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements
Rating: Pass/Fail

- Delivery of screenshots of maps from each mode
- Route maps with descriptions to support map screenshots

Criteria #1: UI/UX Evaluation, Mode 1 Operation
Rating: 20/100

- Subjective scoring of user interface/user experience based on Android Material Design Basics (https://developer.android.com/design/) and Mode 1 mapping presentation.
- Rating (20/100)
  - UI/UX (layout, style, components, patterns, visual quality, Mode 1 presentation): 15/100
  - Mode 1 map performance (coverage data, route accuracy): 5/100

Criteria #2: Mode 2 Operation
Rating: 20/100

- Subjective scoring of Mode 2 mapping presentation.
- Rating (20/100)
  - UI/UX (Mode 2 presentation, ease of interpretation): 15/100
  - Mode 2 map performance (coverage data, route accuracy): 5/100

Criteria #3: Mode 3 Operation
Rating: 20/100

- Evaluation of general application functions and compliance with subset of Android Core App Quality Plan. 10/100
- Subjective scoring of Mode 3 mapping presentation. 10/100
  - UI/UX (Mode 3 presentation, ease of interpretation):
  - Mode 3 map performance (coverage data, route accuracy):

Criteria #4: Final Evaluation — Android Core App Quality
Rating: 20/100

- Assessment of general application functions and compliance with Android Core App Quality test plan (Pass/Fail for all relevant cases https://developer.android.com/docs/quality-guidelines/core-app-quality).
- Evaluation will be performed using a commercial Android UE on a supported Android 9 or 10 build. A successful submission will be able to utilize available sensors from a variety of UEs in order to achieve optimal performance.
- Evaluation of submission summary for compliance with internal requirements (e.g., security, privacy)
- Rating (20/100)
  - Core App Quality test plan: 10/100
  - General application functionality: 10/100

Criteria #5: Final Evaluation — Application Performance
Rating: 20/100

- Comprehensive assessment of application performance.
- Evaluation will be performed using a commercial Android UE on a supported Android 9 or 10 build. A successful submission will be able to utilize available sensors from a variety of UEs in order to achieve optimal performance.
- Rating (20/100)
  - UI/UX (Modes 1-3 presentation, ease of interpretation): 10/100
  - Modes 1-3 map performance (coverage data, route accuracy): 10/100

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- Software application:
  - Android package (APK file)
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
  - A summary of the submission.
  - Screenshots of maps from each mode.
  - Route maps with descriptions to support map screenshots.
  - Basic information about the participant or participant's team.
  - Specific requirements of the contest that are being addressed by the participants.
  - Two to four screenshots of the solutions or prototype.
  - Overview of key functions included in the submission.
- CSV file generated by the application, conforming to the template provided for the challenge.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.5 CONTEST 5: FIRE SAFETY IN 3D: INCENTIVIZING HOMEOWNERS TO CREATE PRE-INCIDENT PLANS FOR FIREFIGHTERS

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Knowing the layout of a home and the resources required when answering a call can save emergency responders precious seconds in an emergency where literally every second counts. Conducting a fire safety inspection in the home can significantly decrease the risk of fire. However, while critically important pre-incident plans and inspections are conducted for commercial or public buildings, residential properties are not subject to these activities. In the last 10 years, over 34,000 civilians and 95 firefighters died while fighting structure fires inside residential properties.

This contest focuses on identifying and demonstrating approaches that incentivize citizens to create fire-safety checklists and pre-incident plans of their homes in a way that is easy-to-use, rewarding, meaningful, and scalable for deploying nationwide. In the next few years, 3D cameras will be common in smartphones, tablets, AR/VR headsets, drones, and robotic appliances. This hardware, along with practically unlimited cloud computing power, will enable homeowners to collect and process 3D scans of their properties and create an unprecedented opportunity to scale a potential solution. With over 121 million occupied housing units in the U.S. alone, this problem is both a tremendous challenge and a massive market opportunity.

1.2 OBJECTIVES

Participants will develop a prototype application that transforms 3D scans collected by users into three outputs: 1) an innovative product or service for the user, 2) a fire safety checklist for the homeowner, and 3) a pre-incident plan for the local fire department. While the latter two outputs are what's important to public safety, the innovative product or service should be the "hook" that incentivizes users to collect and submit the data. In addition to the meaningful fire-safety outputs created by the process, there should also be an engaging purpose to encourage use by homeowners.

For all three outputs, participants are strongly encouraged to exploit the wealth of spatial and image information that is in the 3D data to provide innovative products or services, new insights into residential fire safety, and enable as much automation as possible. Participants are also encouraged to think carefully about the potential business model and ability to scale the approach. There is a wealth of information on the Internet about fire safety checklists and pre-incident plans, however participants are encouraged to engage with their local fire department to understand their most compelling needs. In addition, participants are invited to attend one of the local events to consult with subject matter experts and obtain their input in person.

There are very important questions about how pre-incident information is integrated with local dispatch systems and presented to emergency responders during operations. However, these questions are not the focus of this contest. Instead, this contest is focused on discovering new approaches that will encourage citizen users to willingly collect and share this information, and engage in a more meaningful dialogue with their local public safety organizations.

1.3 RESOURCES

Imagine a future where 3D cameras are ubiquitous, and users will be able to collect and process complex spatial and imagery data very easily using powerful processors in their mobile devices or "the cloud." Participants will be using 3D residential scan data available from the vizHOME project and/or scans collected and provided by PSCR using commercially available 3D cameras (e.g., ZED from Stereolabs, Intel RealSense D435i, Occipital Structure Core).

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

Participants will also use the design and prototyping tools of their choice to create and submit an interactive prototype user interface. Participants should focus their creativity and energy on the more innovative, value-added aspects of this contest, rather than the complexities of designing a working mobile app and interfacing with a 3D sensor to collect and process data.

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements
Rating: Pass/Fail

- Related to Criteria #1-3: The solution demonstrates all three required outputs:
  - An innovative product or service for the user. (Pass/Fail)
  - A fire-safety checklist for the homeowner. (Pass/Fail)
  - A pre-incident plan for the local fire department. (Pass/Fail)

Criteria #1
Rating: 20/100

- This criterion will be evaluated by an in-person demonstration at a codeathon or by using the narrated video.
- **Product or Service:** The extent to which the demonstrated product or service offered to the homeowner is innovative and will incentivize users to scan their homes to generate the fire safety checklist and a pre-incident plan that they share with their local fire department. Further, the extent to which the approach would encourage users to update their information periodically or after major changes, e.g., remodeling.

Criteria #2
Rating: 20/100

- This criterion will be evaluated by an in-person demonstration at a codeathon or by using the narrated video.
- **Fire-safety checklist:** The extent to which the demonstrated fire-safety checklist is innovative, insightful, accurate, and meaningful to homeowners, and will help prevent fires.

Criteria #3
Rating: 20/100

- This criterion will be evaluated by an in-person demonstration at a codeathon or by using the narrated video.
- **Pre-incident plan:** The extent to which the demonstrated pre-incident plan is innovative, insightful, and accurate, and will be useful to firefighters when responding to residential emergencies.

Criteria #4
Rating: 20/100

- This criterion will be evaluated by accessing the required outputs as described in the responsiveness checklist above.
- **Functionality:** The extent to which the required outputs are functionally complete, correct, and appropriate, and return results consistent with those demonstrated in earlier criteria.

Criteria #5
Rating: 20/100

- This criterion will be evaluated by accessing the web or mobile app prototype and required outputs as described in the responsiveness checklist above.
- **User Experience:** The extent to which the prototype demonstrates good user-centered design, a high level of automation (i.e., minimal manual entry required by the user), and the required outputs are appealing and easy-to-understand for both the civilian and public safety users.

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
  - A summary of the submission.
  - Demonstrate the required outputs and provide insight into the design choices that were made.
  - Basic information about the participant or participant's team.
  - Specific requirements of the contest that are being addressed by the participants.
  - Two to four screenshots of the solutions or prototype.
  - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.
- Specific to this contest and in reference to criteria items 4 to 5: a link to a prototype of a web or mobile app created with the prototyping tool of their choice (e.g., InVision, FluidUI, Proto.io, etc.) that enables a reviewer to interact with and evaluate the design as a potential user. This prototype should make it clear to the user what additional data (e.g., number of occupants, type/number of household pets, etc.), if any, is required to create any of the three required outputs. PSCR will provide this additional information, along with 3D scans that will be used for

final evaluation, via a secure file sharing platform (SFSP). The provided 3D scan will be in a format consistent with the data used to evaluate criteria 1-3 below. The SFSP will notify PSCR when the scan(s) have been accessed and downloaded, at which point the participant will have two hours to reply with the processed outputs. Note, there may be multiple scans provided at different times during the final evaluation. The outputs must be available using common file formats/containers, e.g., .jpg, .pdf, .avi, .ply, etc. Participants should contact the challenge team if there are any questions about file formats.

9.6 CONTEST 6: VOICE COMMANDS TO VIRTUAL ASSISTANTS: HANDS-FREE DEVICE CONTROL

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Public safety field operations have challenges with accessing information and controlling equipment in many situations because their hands are not available to control a mobile data terminal, smartphone, or a Land Mobile Radio (LMR). It is paramount that advanced user-interfaces provide "Heads-Up Hands-Free" operation. A law enforcement officer needs to have two hands on their weapon when firing it. They can't afford to have one hand occupied by a mobile device. A firefighter typically has gloves on at the scene, and will also need their hands to manipulate handheld tools and hoses. Again, they cannot afford to have their hands occupied by a mobile device. Finally, an EMS technician needs their hands to treat a patient and manipulate monitoring equipment. There are many instances across the spectrum of public safety where hands-free capabilities can improve the operational efficiency of emergency responders.

A voice-activated virtual assistant could enable capabilities to overcome these challenges. Consumer virtual assistants are becoming widely used for hands-free access to information and device control in very creative ways and this technology could be leveraged for the benefit of public safety. However, because consumer virtual assistants have limitations in the level of customization available to public safety users, a fully customized and optimized virtual assistant may be a very valuable advanced user-interface for public safety users.

USE CASES

The following are typical use cases where an emergency responder would benefit from having access to a virtual assistant:

- *Suspicious Vehicle:* An officer is patrolling an area on foot and needs to identify the owner and history of a suspicious vehicle. The virtual assistant could be used to allow the officer to verbally request the information using the license plate and/or VIN number while maintaining situational awareness (not having to look down at a screen) while maintaining free use of their hands. If they engage with the vehicle owner, they could use a virtual assistant to update dispatch that they have a traffic engagement in progress and to request driver license information. They could also use voice commands to request backup support or the location of other patrol officers in the area.
- *Patient Information:* An EMT or firefighter needs to obtain valuable patient data to provide better care. The virtual assistant would allow the EMT to request information about the patient and it would verbally convey the results. This allows the EMT to maintain use of their hands to administer support to the patient as needed.
- *Commercial Structure Fire:* A fire service team is dispatched to a multiple alarm fire at a commercial building. While in route, the team lead on the fire apparatus uses voice commands to request pre-plan information and previous dispatch history for the address of the fire. A voice command is also used by the team lead to request dispatch details which is read back to the full apparatus team including information on other responding units and their current location. The apparatus engineer uses a voice command to request the route to the dispatch location and a map is displayed within the vehicle showing the route. Additional voice commands can be used to automatically update dispatch or incident status such as leaving station, arrived on site, fire attack active, to rehab, dispatch complete.

1.2 OBJECTIVES

Each participant will be expected to deliver a customized voice-controlled virtual assistant enabled application that can support law enforcement, fire services, and EMS emergency responders. Specifically, the expected solutions could include, certainly not limited to, the following:

- Support of a hierarchical contact list to support communication, location, and status reporting capability to individuals or groups within a public safety authority
- Integration with other virtual assistants to take advantage of their ecosystems
- Support an end-to-end solution including integration with back-end applications and data sources
- Optimized UX for efficient processing of emergency responder command vocabulary along with streamlined dialog
- Ability to function within challenging operational environments
- Provide a user-centered design based on public safety feedback
- Embrace cybersecurity requirements and best-practices throughput the development process (CJIS, HIPAA, etc.)

1.3 RESOURCES

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

In this section, we will provide resources that we believe will be useful to all participants. We have provided resources that give context and structure to the virtual assistant product space, as well as example commercial solutions. In addition, we have provided references to data sources that should be leveraged for this challenge. Finally, we provide a collection of references to SDKs and APIs that we believe would be the foundation for the development of a solution.

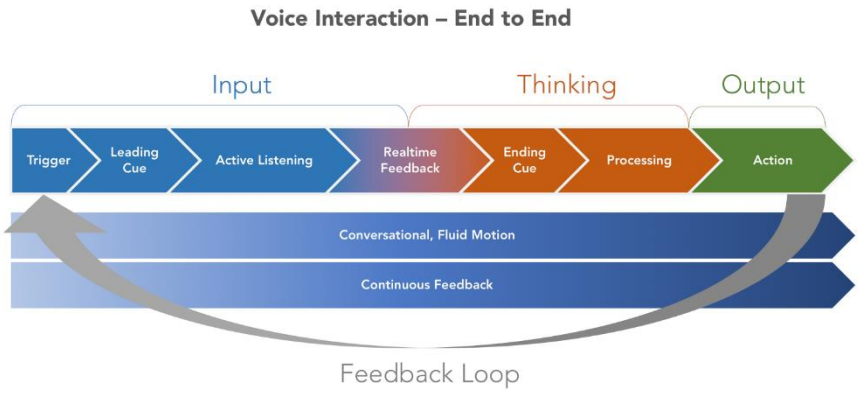


Figure 1. A canonical model for how to organize and manage a system based on voice interaction (https://medium.muz.li/voice-user-interfaces-vui-the-ultimate-designers-guide-8756cb2578a1)

The model shown in Figure 1 represents an approach for thinking about the voice processing structure of a virtual assistant. We provide this as a reference for terminology used in this field and as context for your design.

Commercial Virtual Assistants

These virtual assistants are available to commercial users. We do not view these as "public safety grade" applications, but rather we provide these links to serve as reference locations to foster informed ideation.

- Mastermind: http://www.mastermindassistant.com
- Dragon Mobile: https://www.nuance.com/mobile/mobile-applications/dragon-mobile-assistant.html#standardpage-mainpar_multicolumn
- Hound: https://www.soundhound.com/hound
- Lyra: https://www.heylyra.com/

Data Resources

The following are data resources that should be used by participants to demonstrate an end-to-end integrated solution:

- License Plate Reader Database
- Driver License Database
- Patient Information Database
- Fire Pre-plan and Building Information Database
- Dispatch History

Amazon Alexa

Cross-Platform cloud-based speech recognition for iOS, Android, and Web applications.

- iOS/Android (companion): https://developer.amazon.com/docs/alexa-voice-service/authorize-companion-app.html
- Web (companion): https://developer.amazon.com/docs/alexa-voice-service/authorize-companion-site.html
- iOS/Android (on product — no smart speaker): https://developer.amazon.com/docs/alexa-voice-service/authorize-on-product.html

Apple Siri Kit

Provides cloud-based speech recognition services for iOS applications.

- Main site: https://developer.apple.com/sirikit/
- Developers Documentation: https://developer.apple.com/documentation/sirikit

Open Ears

Provides offline cross-platform speech recognition that can be embedded into iOS and Android applications.

- Main site: https://www.politepix.com/openears/

GOOGLE VOICE ACTIONS

Provides cloud-based speech recognition services for Android applications.

- Main site: https://developers.google.com/voice-actions/
- Developers Documentation: https://developers.google.com/voice-actions/system/

2. EVALUATION CRITERIA

In this section, information is provided about the expected development phases and the evaluation criteria to be used during the duration of the challenge.

2.1 DEVELOPMENT PHASES

The evaluation criteria being applied to the following phases of development throughout the challenge:

- *Phase 1*: Baseline assessment and implementation of core functionality using commercial and/or custom voice assistant and associated artificial intelligence solutions
- *Phase 2*: Optimization for emergency responder vocabulary and efficient access and dialog
- *Phase 3*: End-to-end integration with apps and data sources
- *Phase 4*: Engagement with public safety for assessment and recommendations for optimization of the solution and the preferred support of devices types and associated accessories.

2.2. EVALUATION CRITERIA

The following section provides details on the evaluation criteria and judging areas which will be utilized as part of the challenge evaluation process.

Criteria #0: Core Functionality Checklist (Basic Requirements)
Rating: Pass/Fail

- The solution must provide both a manual and voice prompt (wake word) triggering mechanism to initiate the voice interaction sequence.
- The solution must provide a hierarchical contact list and group management functionality for control of information exchange.
- The solution must provide basic text messaging and email communication capabilities through voice control.
- The solution must provide the ability to exchange location information through voice control.

Criteria #1: Breadth and Depth of Public Safety Skill Development
Rating: 20/100

- The breadth of skill support across each category of public safety users will be assessed against the recommended vocabulary support. These public safety disciplines include:
  - General (common skills used across all disciplines)
  - Law Enforcement
  - Fire
  - EMS
  - Incident Command
- The depth of skill support within a single discipline will be assessed in accordance with the list of recommended vocabulary items.
- Some solutions may provide a wide range of support and others may focus on one discipline for a deep level of support in this area, and the scoring process will accommodate both options.

Criteria #2: Level of Public Safety Customization and Effectiveness in Operational Environments
Rating: 20/100

- Level of customization to provided efficient use within emergency responder operations
  - Streamline the virtual assistant vocabulary and dialog
  - Flexibility to handle a range of utterances for the same intent to minimize amount of user training required
  - Optimized triggering (manual, voice prompt, gesture) and dialog options for seamless and efficient use
  - Capability to interrupt or modify the sequence of a dialog which is in progress
  - Voice command accuracy when operating in challenging noise environments encountered by public safety. The accuracy levels for a range of voice types will be evaluated for the following conditions:
    - Voice command accuracy in nominal environment
    - Voice command accuracy in noisy law enforcement environments (Siren, vehicle noise, large crowd)
    - Voice command accuracy in noisy fire service and EMS environments (Siren/Horn, Chainsaw, Fire Ground, Traffic Accident/Jaws of Life)

Criteria #3: Innovation and Creativity
Rating: 20/100

- Development of innovative and complex skills beyond the items listed in the recommended skill set
- Integration of peripherals providing advanced audio processing capabilities or far field microphone technologies to address challenging operational environments
- Interworking with peripherals within the voice assistant ecosystem including smart speakers, displays, headsets, and other device accessories
- Audio-to-text conversion and language translation support
- Complementary use of other technologies — IoT for equipment control, gesture or other advanced UI capabilities

Criteria #4: Application and Data Integration
Rating: 20/100

- Level of integration with back-end applications and data sources. These may include the following areas of application and data access support:
  - Computer Aided Dispatch (CAD) including dispatch history information
  - Department of Motor Vehicles (DMV) license plate information
  - Driver License Information Database
  - Local, regional, and national criminal history
  - EMS medication data
  - Patient treatment protocols
  - Situational Awareness platforms (location, group status)
  - Support unique security aspects to allow voice control access to sensitive databases and applications. The security concerns fall into the following areas:
    - CJIS for law enforcement criminal database access
    - HIPAA for medical record access
    - Local agency enterprise security requirements
  - Development of sample APIs to support scalable access to applications and databases through voice control

Criteria #5: Emergency responder Usability and Optimization
Rating: 20/100

- Usability of solution to be assessed by public safety personnel in realistic operational and training scenarios
- Optimization of the end-to-end voice interaction process is considered to support:
  - Highly efficient dialog to minimize time to complete voice command actions
  - Streamlined process for data access
  - Flexibility in the range of utterances for the same voice command intent
- Usability improvements and optimizations incorporated to accommodate recommendations from user trials
- The ability of the solution to be demonstrated in a real operational environment with live applications and databases.

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
  - A summary of the submission.
  - Basic information about the participant or participant's team.
  - Specific requirements of the contest that are being addressed by the participants.
  - Two to four screenshots of the solutions or prototype.
  - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.7 CONTEST 7: SENSOR INTEGRATION: MONITORING EMERGENCY RESPONDERS' HEALTH

1. INTRODUCTION

Firefighters, law enforcement officers, and emergency medics have inherently dangerous jobs. Dangers in these occupations are mitigated through rigorous training, processes, and oversight. Dangers manifest themselves through a wide variety of external forces, including gunfire, building fires, and vehicle accidents. An often-overlooked danger is the physical activities emergency responders undertake to do their jobs and the associated stress and exertion those activities place on their bodies. In 2017, 87 firefighters died in the line of duty. Of those 87 deaths, 52 were the result of stress or overexertion; this includes all deaths that are cardiac or cerebrovascular in nature, such as heart attacks and strokes, as well as other events, such as extreme climatic thermal exposure.[6] Similarly, 139 law enforcement officers died in the line of duty in 2017; 16 of those officers died of a heart attack.[7] Technology in the realm of personal biometric health and wellness sensors has advanced dramatically over recent years. Many people today wear basic health monitoring devices in the form of smart watches and workout sensors. Leveraging health and wellness biometric sensors for emergency responders and combining data obtained from them with other relevant data for firefighters (e.g., air reserves, temperature, location, presence of hazardous materials and gases) and law enforcement officers (e.g., unholstering a weapon, body cameras, location) can result in fewer deaths.

1.1 PROBLEM STATEMENT

- Emergency responders need a tablet- or smartphone-based dashboard showing the status of sensors worn by emergency responders or sensors connected to the equipment they use. Multiple technological solutions (sensors) exist in both the public safety and consumer markets today to monitor the health of emergency responders and to monitor their activities and equipment. However, most of these solutions are limited in their ability to serve the emergency responder needs for the following reasons:
    - Narrow focus and single-dimensional solution that solves only a subset of the many issues faced by emergency responders.
    - Use of proprietary mechanisms and data formats that do not scale and fail to integrate with emergency responder systems.
    - Data processing and presentation capabilities lacking in their support of real-time, high-intensity decision making faced by emergency responders and their supervisors.
    - Generalized solutions not specific for use by an emergency responder discipline (law enforcement, fire and EMS).

USE CASES

- Structure Fire — During a structure fire, firefighters face environments with temperatures of hundreds of degrees while wearing and carrying more than 50 pounds of equipment, crawling through low visibility in an environment full of noxious gases, and strenuously exerting themselves. Monitoring heart rate, blood pressure (BP), temperature, and air supply allows supervisors to determine when a firefighter needs to be removed for his or her own safety. In the event of an emergency, location data would allow for efficient rescue.

[6] https://www.usfa.fema.gov/data/statistics/ff_fatality_reports.html

[7] https://www.odmp.org/profile/login?referral=https%3A%2F%2Fwww.odmp.org%2Fstatistics

- Foot Pursuit — During a foot pursuit, supervisors and dispatchers could simultaneously monitor a law enforcement officer's location and heart rate via a system of sensors to accurately deploy backup units or provide medical attention for the officer, if needed.
- Hazardous Material Incident — During a hazardous materials response, emergency responders operate in immediate dangerous-to-life and -health environments while wearing chemical protective clothing that adds significant stress to the responder. Their attire limits movement and situational awareness, as well as increases heat. Access to internal and external cameras, biometrics, chemical metering devices, and nearby unmanned devices are used to address these incidents.
- Other — Emergency responders in many other situations, including traffic stops, active shooter incidents, wild fire fighting, and day-to-day custodial responsibilities, to name a few, would benefit from remote monitoring of various on-body sensors for overall safety and awareness.

1.2 OBJECTIVES

The desired dashboard solution will address the issues listed in the problem statement and assist with monitoring and tracking the health and safety of emergency responders. A mobile application should be developed, including appropriate datasets, sensors, consolidation of data, and other UI/UX elements to demonstrate a solution relevant to the problem statements and use cases.

Note: While the desired solution would connect across the FirstNet cellular LTE or a similar network, participants should not assume availability of LTE coverage and should be prepared for sensors connected via a mesh network, Wi-Fi, or other capability.

1.3 RESOURCES

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

SENSORS

- Body-worn video cameras
- Self-Contained Breathing Apparatus (SCBA) monitors
- PASS (Personal Alert Safety System) for Firefighters
- Gas meters and monitors; radiation monitors
- Thermal imaging cameras (plus night vision, etc.)
- weather stations and other temperature/weather monitors (e.g., temperature, wind speed, barometric pressure, humidity)
- Personal Biometric devices
- Radiation monitors
- Other gas monitors non-VOCs metered by a PID — LEL, CO, O2, H2S, CL2, NH3, etc.
- Night vision cameras
- Apparatus network or sensor feeds, such as pump pressure output and air pressure

DATASETS

- https://registry.opendata.aws/
- https://data.austintexas.gov/Public-Safety/Indicator-EMS-Overall-Response-Fleet-Maintenance-b/j7an-ra5x/data (can be exported in a file)
- https://edg.epa.gov/metadata/catalog/search/resource/details.page?uuid=%7BCE289244-BF45-40F3-867E-B2D691018D34%7D
- https://catalog.data.gov/dataset?groups=disasters#topic=disasters_navigation(NOAA)
- https://dromic.dswd.gov.ph/about-us/ (Disaster Response Management Bureau)
- http://opentopo.sdsc.edu/datasetMetadata?otCollectionID=OT.072010.32618.1(World Band Haiti EQ datasets)
- https://www.sciencebase.gov/catalog/item/4f70b240e4b058caae3f8e1b (USGS National Structures dataset)
- https://catalog.data.gov/dataset/usgs-national-transportation-dataset-ntd-downloadable-data-collectionde7d2 (USGS National Transportation dataset)
- https://data.humdata.org/search?q=Ebola (West Africa Ebola breakout)
- https://www.fema.gov/openfema-dataset-openfema-data-sets-v1 (FEMA)
- https://registry.opendata.aws/ (AWS open datasets)

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements
Rating: Pass/Fail

- Item 1 (Pass/Fail) — Application's ability to display or communicate the responder's location(s)
- Item 2 (Pass/Fail) — Participant's submission can be effectively deployed for use with a tablet computer or smartphone as the user's device
- Item 3 (Pass/Fail) — Application's ability to display outputs from at least one sensor

Criteria #1: Sensor Identification
Rating: 20/100

- Application's ability to identify and display data from at least one health and wellness sensor and/or environmental data and/or hazardous material data and/or emergency responder equipment data usable by emergency responders

Criteria #2: Data Aggregation
Rating: 20/100

- Application's ability to appropriately identify relevant data from multiple different sensors belonging to a single emergency responder and/or attached to multiple emergency responders and determine how to aggregate relevant data to provide assessment of emergency responder health and operations

Criteria #3: User Interface (UI)
Rating: 20/100

- Application's user interface, design, and capabilities relevant to the use cases for a user to see and interact with sensor data from emergency responders on an incident

Criteria #4: Configurable Thresholds, Alerting
Rating: 20/100

- Provide a proactive alerting functionality within the application when sensor data indicates an unhealthy situation for an emergency responder.
- Allow application user to set trigger thresholds for incoming data via an interactive dashboard.
- Allow for responder evacuation alerting, which means a high priority audible, haptic, and/or video alert sent to any connected device which can receive it.

Criteria #5: SDK/API
Rating: 20/100

- Provide an SDK to support expansion and customization that integrates data from selected relevant sensors.
- Provide an API to support interoperability and allow the data collected to be shared across hardware platforms, applications and locations on site or via remote servers. These applications might be a records management system, computer-aided dispatch system, or a similar application.

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

1. A completed submission form through www.techtoprotectchallenge.org
2. Mobile friendly application with the following minimum functionality:
    a. Provide the ability to configure emergency responder sensors and sensor networks if and as needed
    b. Integrate emergency responder biometric health and wellness data with data from specialized sensors and other sources (e.g., air tank supply monitors, hazardous materials sensors, weather stations, body worn cameras, thermal imaging cameras)
    c. Provide a dashboard with real-time location-based information (processed data) regarding current location and health status of the emergency responder in a given emergency event
    d. Provide configurable alarms with visuals on dashboard when sensor information determines signs of risk to emergency responder safety and health.
3. Any available files or links to the developed solution or prototype.
4. A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
    a. A summary of the submission.
    b. Basic information about the participant or participant's team.
    c. Specific requirements of the contest that are being addressed by the participants.
    d. Two to four screenshots of the solutions or prototype.
    e. Overview of key functions included in the submission.
5. Documentation of the solution including:
    a. High-level roadmap to commercialization of the solution and an SDK (if applicable).
    b. Challenges to commercialization.
6. Brief report of the contest experience of the participants.
7. Any additional files based on the contest description.

9.8 CONTEST 8: NO COVERAGE: PLACING DEPLOYABLE NETWORKS IN EMERGENCIES

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Broadband coverage is going to be, and may already be for some, the gold standard for what an emergency responder needs as a technology. Broadband connectivity allows for more complex and useful information to be conveyed so that emergency responders can carry out their daily duties more effectively. A problem arises in how to provide them with this technology everywhere and at all times. The solution is a deployable system, which in simple terms is a portable box that can provide broadband services to everyone on scene.

USE CASE 1: WILDFIRES

Let's start with a scenario to help our understanding: Picture yourself as a firefighter in a National Forest trying to contain a burn area of several hundred acres. You are in the woods with no access to a live map of where you are, no voice or text communications from your cell phone to others in the area, and no access to services like video feeds that could be covering the fire. A deployable system can provide all these services and more depending on the needs of each agency.

USE CASE 2: NATURAL DISASTERS

This is not limited to spot cases like wildfires, either. Imagine being a law enforcement officer on the Gulf Coast where a hurricane just came and knocked down multiple cell towers in the area. Your only link to others is your trusty old push to talk radio, but that device has some limitations. The radio cannot tell you where all your fellow officers or medical units are in the area, nor could you upload video and critical data intensive information to anyone around you. It's absolutely trustworthy and still a great tool, but we can provide more to our emergency responders.

Solutions to both cases and many more exist today in the form of a deployable system, but they face many challenges, both policy-wise and technically for public safety to use. One roadblock public safety faces is the lack of operational understanding of what these systems can do. This challenge contest is to build a solution that will help emergency responders understand what these systems can do for them in terms of coverage and service usability.

1.2 OBJECTIVES

The objective of this contest is to enable participants to create prototype network diagnostic tools to help emergency responders understand what coverage a broadband deployable system can provide. Participants will be able to leverage their knowledge of computer systems, RF, common sense, user interface design, and other relevant skills in order to accomplish this.

The end goal is to let emergency responders use the app to let them know:

- What's the **expected** coverage area?
- What services can I **expect** out at specific locations?
- What's the **real**, measured coverage?
- What's the **real** service quality at specific locations?

1.3 RESOURCES

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

1. Participants will have at their disposal a few example datasets from a real deployment of a deployable system. These datasets will serve as a reference to help tune participant solutions.
2. A range of what the deployable system characteristics could be, for example a range of the possible output powers and antenna types, will be provided to participants.
3. Participants will receive an estimated translation table for coverage quality to usability for text, voice, and video.
4. Participant can also use open source RF propagation software such as SPLAT! and Qrap as well as some simple open source propagation models. Participants are not required to use these in their submission.
   https://www.qsl.net/kd2bd/splat.html
   http://www.qrap.org.za/
   https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.529-3-199910-W!!PDF-E.pdf
   https://www.its.bldrdoc.gov/resources/radio-propagation-software/itm/itm.aspx
   http://qradiopredict.sourceforge.net/

2. EVALUATION CRITERIA

CRITERIA #0: BASIC REQUIREMENTS
RATING: PASS/FAIL

- The solution must provide an expected coverage area of a deployed LTE system. Specifically, it must provide a heat map, overlaid on a real map, that reflects LTE Reference Signal Received Power (RSRP) measurements.
- This map must be interactive, meaning the deployable systems characteristics can be changed and the outputs are automatically updated.
- The solution must provide expected services at any location from the deployable system. Specifically, participants are required to provide some indication of the usability of text, voice, and video services. How this information is conveyed is up to the participant.
- The solution must update the expected coverage area with measurements from user equipment in the field. This provides emergency responders with the "current real coverage" in the areas where measurements are taken. Specifically, it needs to take in GPS vs RSRP and update its coverage map accordingly.
- The solution must update the expected services at locations with measurements from user equipment. This provides emergency responders with the "current real services" that are available in the areas where measurements are taken.
- The solution must provide data of dead spots or areas without any connectivity. More specifically this is anywhere a phone cannot connect to the network or if the predicted RSRP strength is lower than -140dbm.
- The solution cannot rely on any cloud services and must be local at all times. This is to simulate a real deployment.

CRITERIA #1: EXPECTED COVERAGE AND SERVICES
RATING: 20/100

- Expected coverage (15/100)
    - This will be objectively scored based on a submitted CSV file that the participant will upload near the end of the competition. We will compare your predicted RSRP values, on a specified deployment scenario, with what we measured from a real deployable system.
- Expected services (5/100)
    - This will be objectively scored based on the same submitted CSV file. We will check to see if you implemented the RSRP to service translation. Even if your RSRP predictions are not consistent with our data, did you at least include and provide a service translation.

CRITERIA #2: CURRENT COVERAGE AND SERVICE
RATING: 20/100

- Current coverage (20/100)
    - This will be objectively scored based on another CSV file submission at the end of the competition. We will provide you with a partially filled in CSV file with only some data points of the same deployment scenario. From their your solution should be able to make improvements from its initial prediction. Think of this as now incorporating an interpolation function. You will then submit a completely filled out CSV file that we will grade again in the same way as before. This will take place an hour before the competition ends.

CRITERIA #3: WILD CARD AND FEATURES
RATING: 20/100

Participants may include added functionality that enhances the value of the solution in the context of the use cases provided. These points will be given by our judges at their discretion. They will be looking for incredible and unique ideas that make your app different from the rest. Think about what an emergency responder might need to know or what another developer could do with your solution. You could build an API framework into your solution or have added features like Wi-Fi coverage prediction and measurements. Think about some of the other bits of information a smart phone can provide like throughput and latency between points; see if you can use those in a clever way. You could also develop an entire architecture around features that you may not have time to implement.

What will happen here is your submission will include a short Word document (300 words at most) that describes the added features you think qualify for this category. You can reference screenshots that you submit to further explain what the feature is. You will submit this document and the screen shots at the close of the competition.

CRITERIA #4: USER INTERFACE/USER EXPERIENCE
RATING: 40/100

This score will be based on subjective judgements made by a panel of public safety and technical experts to evaluate the User Interface and User Experience (UI/UX) of the solution. Not all users will make it to this section as only qualifying submissions from the last two scoring sections will be graded. In essence, users are pushed to make a solution that conveys information in an easy-to-understand format without any substantial user training. For additional information on UI/UX[8], below is a breakdown of what would be considered a good UI/UX:

A good one conveys information in a usable manner after training.
(0-10 points based on judges)

A great one conveys information in an easy way after minimal training.
(10-25 points based on judges)

An excellent one conveys information in an easy way without any training.
(25-40 points based on judges)

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

3.1 CONTEST SPECIFIC DELIVERABLES

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

Part 1

Output:

- Specific to this contest, participants will be provided an example deployment configuration and some GPS coordinates. Participants will run their solution with this configuration information and fill out the CSV file with the RSRP and service usability for the GPS points provided. This output is the expected coverage and service usability for the participant's solution.

Process:

- 4 hours before the end of the contest, a CSV file, which can be found at www.techtoprotectchallenge.org, will be available to all participants and it will contain specific deployable characteristics and GPS coordinates around the deployable system. You will submit an example screenshot of your code and the same CSV file, but filled out with RSRP and service expectation at each point. You will only have 2 hours to complete this task, so make sure your solution is working by the time the CSV file is released to you.

[8] https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&limitstart=0

Part 2

Output:

- In order to see if your solution takes in real measurements, we will repeat the procedure above but with new points and some real measured points. Your solution should now have a better coverage map given some real points. This is the real coverage and service usability for your solution.

Process:

- Approximately 2 hours before the end of the competition, we will provide another CSV file, which can be found at www.techtoprotectchallenge.org. This file will contain the same deployable characteristics as before, but the twist is that we will include completely different GPS points. Some of those points will have real measured RSRP values included You are to input this new CSV file into your solution, with real measurement points, and fill in the rest of the blank points. You will only have 2 hours to complete this task and upload your solution's completed CSV output, so make sure your solution is working by the time this CSV file is released to you.

3.2 ADDITIONAL DELIVERABLES

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
    a. A summary of the submission.
    b. Basic information about the participant or participant's team.
    c. Specific requirements of the contest that are being addressed by the participants.
    d. Two to four screenshots of the solutions or prototype.
    e. Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.9 CONTEST 9: MAKING THE CASE: PROACTIVE IMAGE PROTECTION

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Digital photographs provide powerful and impactful evidence for law enforcement and the courts. However, advanced photographic manipulation techniques and capabilities have elevated concerns about integrity and provenance. Emergency responders need a proactive solution: a smartphone camera app and verification tool that work together to prove image integrity and provenance.

- Image integrity — whether the image has been altered after being generated
- Image provenance — proof concerning the origin of an image and how it was created (e.g., when an image was taken, what device was used to capture the image, and where the image was taken)

USE CASE: Evidence Provenance

Investigators are responding to the scene of a forced entry. Using an app on their officially issued mobile devices, they capture images of the scene. These images are entered into evidence in both their investigation and the ensuing court case against an accused perpetrator. Anyone who receives the images can run the verification tool to establish where and when the images were taken, the vendor and model of the smartphone, and whether the images were altered. Because law enforcement can provide proof of both the provenance and integrity of the images taken at the crime scene, their case against the accused is strengthened against accusations of image tampering and forging.

1.2 BACKGROUND

Protecting Image Integrity

Image tampering is a problem for the courts. Increasingly robust software allows people to make subtle changes to photos that are difficult to detect (e.g., change faces, add a gun, or remove tattoos). There are many ongoing efforts to solve this problem from the forensic end of this problem. For example, DARPA is working on challenges that address this problem from the viewpoint of inspecting images (i.e., pixels, compressed images)[9]. These algorithms do the equivalent of looking at an image to find tampering. This is a reactive solution. Our challenge contest seeks a proactive solution instead.

Early attempts at a proactive solution met with resistance. See for example the Wikipedia discussion of digital watermarking cameras (https://en.wikipedia.org/wiki/Digital_watermarking/). Solutions that alter images within the camera may be viewed as confidence reducing alterations. Law enforcement and the courts must be able to understand the solution before they will trust and use it.

Naive solutions involve the use of *cryptographic hashing* to provide proof of image integrity. However, the promulgation of these hash artifacts requires an infrastructure to ensure their proper use.

[9] https://www.darpa.mil/program/media-forensics

Providing Image Provenance

Digital evidence collection should be a rigorous as its analog counterpart. Consumers expect large drops in quality when moving from DSLR cameras to compact cameras to phone cameras, but in reality, the quality drops are small[10]. Digital smartphones are commonplace multi-purpose tools that public safety can leverage to bolster confidence of photographic evidence as authentic and trustworthy. In this context, image provenance means being able to prove certain characteristics concerning the source of a given image. This includes, but it not limited to:

- The physical mobile device used to capture the image, represented either as a MAC address, IMEI, or another unique device identifier
- The physical location (GPS, connected cell tower, etc.) of the device when the image was captured
- The time at which the image was captured
- The department's identifying information (e.g., department name, case number)

1.3 OBJECTIVES

The goal of this contest is to build a system that provides Proactive Image Protection (PIP) for a photo taken by a mobile device. This system will be referred to as *the PIP solution* or *the solution*. A photo that adheres to the following requirements will be referred to as a *PIP image:*

- Image integrity — whether the image has been altered after being generated
- Image provenance — proof concerning the origin of an image and how it was created (e.g., *when* an image was taken, *what* device was used to capture the image, and *where* the image was taken)

There are three primary deliverables involved in answering this contest:
- A solution pitch with an overview of the proposed approach
- A mobile app that generates PIP images
- A verification tool that examines images and proves PIP

Please reference section 3. Expected Deliverables from Participants for further details about these deliverables.

[10] https://www.its.bldrdoc.gov/publications/2820.aspx and https://www.its.bldrdoc.gov/publications/3172.aspx

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements
Rating: Pass/Fail

- Participant submission meets the parameters specified in section 3.1 Deliverable #1: Solution Pitch (below).

Criteria #1: PIP Pitch
Rating (20/100)

These criteria assess whether participants understand the challenge. Using the PIP pitch described in deliverable #1, a public safety official will assess whether the PIP solution:

- Can be understood
- Is proactive
- Seems plausible and inspires confidence
- The PIP solution cannot store images on a system external to the mobile device.
- Does not modify the images in a way that may be perceived as corruption or distortion
- Public Safety can afford any required infrastructure

Criteria #2: Cybersecurity
Rating (20/100)

These criteria assess core functionality of the PIP solution.

- The PIP solution will operate correctly when mobile access is unavailable, though operating without network may affect the confidence of the provenance of the image (airplane mode)
- Does the app prompt the user to choose a camera app to take the picture (Pass/Fail)?

Criteria #3: App & Verification Tool User Interface
Rating (20/100)

These criteria assess the mobile app and verification tool.

- The judges can use the app to take a photograph
- The judges can copy the PIP images from the smartphone to a laptop
- Participants demonstrate verification failure (e.g., take a PIP photo, alter it with a hex editor, show that the image fails the verification check)
- The images generated by the app are standard JPEG files (e.g., jpeg or jpg extension, viewable by image viewers, image editors, and word processors)

Criteria #4: Advanced Cybersecurity
Rating (20/100)

These criteria provide an in-depth assessment of the PIP solution's cybersecurity, performed by SMEs.

- The PIP solution is technically sound
- The PIP solution does not raise concerns as a forensic evidence tool
- Supporting metadata generated by the PIP solution cannot be used to re-create the original image
- Technically sound strategies are used to create optional data (e.g., accuracy of date and time, accuracy of geolocation)
- PIP images that are altered fail their verification check. When the judges run the verification tool, the PIP information on app and verification tool match
  - *when* an image was taken
  - *where* the image was taken
  - *what* device was used to capture the image
  - *whether* the image was modified
  - *which* department took this photograph and for *what* purpose
- And, optionally
  - *how accurate* is the date and time?
  - *how accurate* is geolocation?
- Any supporting information that is crucial to the PIP solution (other than the actual images) should be protected if they stay resident on the device.
- If the PIP solution relies on network communication, it must implement Transport Layer Security (TLS) properly
- The app adheres to the subset of the NIAP Protection Profile for Application Software[11] required for this competition.
- The app avoids the OWASP Mobile Top 10 security vulnerabilities[12]

Criteria #5: User Experience
Rating (20/100)

These criteria provide an in-depth assessment of the user experience, performed by SMEs.

- The app installs and runs on at least one of the following devices: iPhone XS Max, Sonim XP8, and Motorola LEX L11[13]
- The app adheres to consumer expectations around a camera app (e.g., JPEG/JPG images, point-and-click, images and data easily transferred to and used by other devices and software)
- The workflow is easy to use (e.g., will minimize user error)
- The app provides excellent quality of experience (QoE)
- The PIP solution will scale to thousands of users and devices

[11] https://www.niap-ccevs.org/Profile/Info.cfm?PPID=394&id=394

[12] https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[13] https://www.firstnet.com/marketing/index.html#/marketing/index/devices/phones

- The PIP solution provides good image quality
- The PIP solution pitch describes a unique and innovative strategy that may appeal to departments that are dissatisfied with other solutions (e.g., due to unforeseen policy concerns)
- Satisfies multiple public safety use cases (e.g., law enforcement, EMS)
- Verification of PIP images is accessible to the greatest number of users at minimal cost to them

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

3.1 Deliverable #1: Solution Pitch

Participants must describe their overall solution to the challenge statement. The solution pitch must contain the following:

- A high-level description of the PIP solution. This description should highlight the technical model, workflow, and/or algorithms used to create PIP images as well as how PIP verification integrates into this workflow.
- Description of how the solution will enable users in heterogeneous environments to verify PIP images (e.g., prosecution and defense teams).
- Specific information on the following security concerns:
    - How the app will protect any sensitive data generated by the app at rest (stored in permanent storage) on the device
    - How the app will protect any sensitive data generated by the app that is transmitted off the device
    - How the participants approach code quality and best practices for design
    - How the verification will protect any sensitive data
    - How the verification will prove PIP

The solution pitch can either be:

- A written document, not to exceed two pages
- A slide presentation, not to exceed 10 slides
- A narrated video, not to exceed 3-5 min

3.2 Deliverable #1: Mobile App

Participants must create a working camera app with the following functional characteristics:

- The app must run on at least one of the following devices: iPhone XS Max, Sonim XP8, and Motorola LEX L11
- The PIP image must be a standard JPEG file
- The algorithm(s) used to establish PIP must be transparent (that is, they must be describable to activity judges).
- The PIP solution must not make images available to a third party
- Metadata that is part of the PIP solution cannot be used to re-create the original image

- The app must use strong cryptographic methods including, if using network communications, network transport security
- The user interface must adhere to consumers' expectations around camera apps (e.g., easy to use and images can be viewed with the smartphone's default image viewer)
- Competition judges can retrieve images from the smartphone via USB or via a network transfer
- The PIP images may be viewed with any JPEG compliant software
- The app must not use other camera apps to take the pictures (this because, we cannot be sure to the security standing of the other camera apps)

The following characteristics are desirable but not required:

- The PIP solution establishes geolocation with accuracy (e.g., plus or minus 100 feet vs. 0.5 miles)
- The PIP solution establishes calibrated date and time, with due diligence proving accuracy (see ANSI X9.95)
- The PIP solution includes advanced planning for forensic image post-processing that is beyond the scope of this challenge (e.g., forensic image enhancement software takes a PIP image, applies auto-contrast corrections, redacts faces, and saves the modified image as a new PIP image that specifies the processing chain)

3.3 Deliverable #2: Verification Tool

Participants must create a verification tool (e.g., software package or website). The verification tool does *not* need to be publicly available when the PIP solution is submitted. The verification tool must have the following functional characteristics:

- When given a PIP image, provides PIP information
- Otherwise, indicates that PIP cannot be established (e.g., PIP image has been modified, JPEG file is *not* a PIP image)
- The verification tool should be able to run on a laptop running Windows 10 or Ubuntu 18.04
- Is easily operated by naïve users

3.4 Additional Deliverables

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections (this should be an updated version of the video or complimentary to the deliverable for 3.1):
    - A summary of the submission.
    - Basic information about the participant or participant's team.
    - Specific requirements of the contest that are being addressed by the participants.
    - Two to four screenshots of the solutions or prototype.
    - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.10 CONTEST 10: ORGANIZING CHAOS: CALMING CATASTROPHE BY TRACKING PATIENT TRIAGE

1. INTRODUCTION

1.1 PROBLEM STATEMENT

During mass casualty incidents (e.g., multiple injury vehicle accidents, mass shootings), emergency medical services (EMS) personnel must quickly assess the severity of each victim's condition and assign each person a priority for immediate treatment. Today, this information is captured via a paper "tag" or card system; see Figure 1. We are asking for more advanced technology to be applied to this process to increase efficiency, expedite the process and, ultimately, save more lives. Patients' status must also be captured and tracked from the initial call through treatment, transport, and discharge to receive proper care, as well as to identify how EMS systems can be improved after each event. Patient tracking also allows Incident Commanders (IC) and hospital staff to map patient locations and understand an event's severity in real-time to improve incident management. You could help fill this vital need for improved emergency management and patient care by developing technology that streamlines the process and assists with capturing evidence that would inform potential changes to local and national EMS protocols.

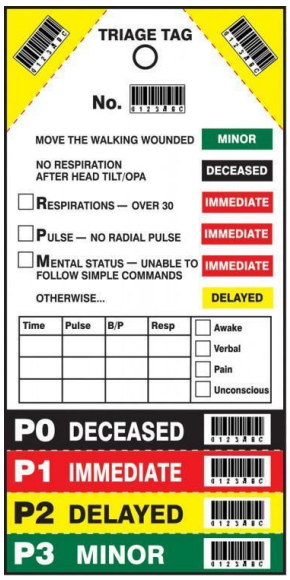


*Figure SEQ Figure * ARABIC 1. Triage Tag.*

Mass casualty incidents create chaotic scenes with injuries ranging from fatal to "the walking wounded." The first EMS team to arrive on scene must immediately triage the patients; triage is the sorting of patients by priority for treatment, evacuation, or transport. This involves locating all the injured, conducting a quick assessment, and then "tagging" them in a way that indicates the injury's severity and the urgency of getting follow-up treatment. This operation is critical to saving as many lives as possible without wasting time on fatal or minor injuries; "to optimize overall patient outcomes in a catastrophic situation, there is a shift from doing what is best for the individual patient to doing the greatest good for the largest number of people."[14] Today, this happens by using a paper form and tag that is completed by hand and attached to the patient with string.

USE CASES

Mass casualty incidents are defined as situations that place a significant demand on medical resources and personnel. Local response capabilities are not overwhelmed; however, there are still a large number of patients requiring triage.[15] Use cases relevant to this challenge are as follows:

- Multiple Vehicle Accidents — During a rain-soaked commute, a 20-car pile-up occurs on the local interstate. The first EMS team on the scene must locate all vehicles involved, victims in those vehicles, and those ejected or wandering. They must quickly assess the injuries and tag each victim for priority treatment.
- Mass Casualties after Bombing — Through the news and social media, many of us are familiar with the images of the aftermath of the Boston Marathon bombing. The EMS teams already on

[14] https://journalofethics.ama-assn.org/article/disaster-and-mass-casualty-triage/2010-06

[15] Ibid.

scene for the race had to locate victims in and around the location of the blast, assess injuries, and tag each victim for priority treatment and transport.

- Mass Shootings — Victims of a mass shooting in a school, mall, or outdoor venue have to be identified and a quick assessment done of the severity of their injuries. Gunshot wounds are often difficult to assess because of the internal damage that is not obvious.

1.2 OBJECTIVES

Provide EMS with an alternative method for locating, tagging, and tracking patients in mass casualty incidents.

- Potentially use patient's smartphone or smart watch (e.g., Fitbit, Apple Device) to locate and identify victims and to provide medical data, name, address, doctor, and next of kin, as well as to populate forms
- Possibly leverage disposable RFID tags (e.g., wrist bands, adhesive tags with QR codes) combined with a simple smartphone application that records initial assessment and allows for expansion as additional treatment and transport is provided
- Solutions should be simple and user friendly, leverage existing industry standards, and adequately address relevant HIPAA concerns

The expected solution is an application that can record a patient's initial condition and generate a physical artifact that remains with the patient to inform follow-on care providers. The physical artifact may be a tag of some kind (e.g., RFID wrist band, adhesive decal, QR code) or a virtual marker that follow-on responders can view and update with additional information. Data input would include patient identification, description, vital signs, initial assessment, location, and triage status (i.e., deceased, immediate, delayed, minor). The application should also provide a dashboard display that summarizes all patient data by severity for Incident Command and hospital notification.

1.3 RESOURCES

The resources for each contest are provided for informational purposes only and include basic information or data to assist participants with getting started. The resources are provided "AS IS" and NIST makes NO WARRANTY OF ANY TYPE. These resources will be provided via the challenge website and will be open access to all registered participants for use in preparing their submissions. Any mention of commercial products, data sets, or other resources within this document is for information only; it does not imply recommendation or endorsement by NIST.

- Challenge team will provide sample mass crisis scenarios with sample patient data.
- PSCR will provide FirstNet compatible devices (e.g., smart phones, tablets) that can be loaded with participant applications for testing and demonstration purposes.
- Challenge Team will provide links to current Triage systems in use today.
- Challenge Team will provide links to HIPAA requirements.
- Any solution should be consistent with and support the Model Uniform Core Criteria for Mass Casualty Incident Triage (MUCC).[16,17]
- Solutions should adhere to EDXL Tracking Emergency Patient v1.1 standards developed by OASIS[18]

[16] Friese, Greg. "How to standardize mass casualty triage systems." EMS1.com, March 5, 2018. Available online.
[17] Lerner, E. Brooke, et. al. "Mass Casualty Triage: An Evaluation of the Science and Refinement of a National Guideline." Disaster Medicine and Public Health Preparedness, June 2011, Available online.
[18] OASIS. "EDXL Tracking of Emergency Patients (TEP) v1.1 from Emergency Management TC approved as a Committee Specification." October 11, 2018. Available online.

2. EVALUATION CRITERIA

Criteria #0: Basic Requirements
Rating: Pass/Fail

- The solution must have the ability to "tag" a patient with initial assessment data
- The solution must generate a physical or virtual artifact that remains with the patient
- The solution must capture patient's current location
- The solution must allow for updates to patient data as treatment and transportation are performed

Criteria #1: User Experience
Rating: 20/100

- The solution is easy to use and intuitive for EMS providers.

Criteria #2: Security
Rating: 20/100

- The solution offers enhanced security so only authorized personnel can view data.
- Note that if the solution is to be considered for actual deployment, all provisions of HIPAA and MUCC criteria must be addressed by the Participant.

Criteria #3: Functionality
Rating: 20/100

- The solution provides easy to view and consume summary patient/victim data (e.g., dashboard format) to IC and hospital staff.

Criteria #4: Integration
Rating: 20/100

- The solution automatically transfers data to existing electronic patient care reporting (ePCR) tools.

Criteria Item 5: Alerting
Rating: 20/100

- The solution can send an alert to EMS if patient condition worsens (e.g., full arrest).

3. EXPECTED DELIVERABLES FROM PARTICIPANTS

Review the How to Participate instructions in section 3 of this document to ensure that you are prepared for the in-person Regional Codeathon or Online Contest. The following deliverables will need to be included with the submission:

- A completed submission form through www.techtoprotectchallenge.org
- A 3-minute narrated PowerPoint file or 3-minute narrated video with the following sections:
    - A summary of the submission.
    - Basic information about the participant or participant's team.
    - Specific requirements of the contest that are being addressed by the participants.
    - Two to four screenshots of the solutions or prototype.
    - Overview of key functions included in the submission.
- Any available files or links to the developed solution or prototype.
- Any additional files based on the contest description.

9.11 CONTEST 11: NATIONAL AWARD EVENT CONTEST

1. INTRODUCTION

The National Award Event Contest is the final round of awards in this challenge. Participants selected in the Online Contest will be invited to the National Awards Event. Participants will prepare for a live pitch session as part of a NIST-managed public event, Demonstration (Demo) Day, to showcase their solution, market entry and scale-up strategy, and a 6-month growth plan. During Demo Day, participants will be evaluated by judges appointed by the NIST Director and judged in accordance with the evaluation criteria specific to this contest. This contest consists of three rounds: Demonstration Round, Seed Round and Progress Round.

2. OBJECTIVES

The National Awards Event Contest is focused on recognizing the technical expertise of participants and providing initial resources to support participants on the path to further development and potentially to commercialization. These resources are not intended to support the full cost of commercialization. They are seed funds to support the first steps and progress towards the goal of commercialization. NIST PSCR's objective is to demonstrate cutting edge technologies developed by participants, engage the public safety community, and connect participants with public and private follow-on resources — mentorship, potential customers, financial investment, and other resources to support participants beyond the end date of the Tech to Protect Challenge.

3. RESOURCES

Selected participants will be responsible for completing their preparations for the National Awards Event within the time frame provided by NIST PSCR. This time frame will be provided to participants with their selection notice and invitation information in January 2020. The event is expected to be held in April 2020.

NIST PSCR may support domestic travel within the Continental United States for up to two individuals for each selected participant or team of participants to attend the National Awards Event in person. NIST may at its discretion arrange and pay for the travel or provide a cash award to support travel for these selected participants. NIST will facilitate at least two preparation webinars for all participants to understand the preparation requirements, schedule, evaluation criteria, and other logistical aspects of National Awards Event Contest.

4. HOW TO PARTICIPATE

Visit http://www.techtoprotectchallenge.org/ and follow instructions to submit the required material for the National Award Event Contest by the deadline. Participants selected will use the same access name and password, and must submit their information and documents by the deadline.

At the National Award Event, each participant will be scheduled to demonstrate their submission to a panel of judges in real-time for 15 minutes, discuss the market entry execution strategy, and the 6-month growth plan. Judges will be able to ask clarifying questions during these 15 minutes to make a well-informed assessment of each participant's submission. Judges will score the content before inviting the next contestant to begin. After all of the presentations, the Judge Panel will convene and discuss all applications and give their final scores in accordance with the review criteria. An official from NIST will announce the winners.

The National Award Event participants will be eligible to compete in the demonstration round and the seed round. Participants in the progress round will be limited to those selected in the seed round only**.** For the participants in the seed round to be eligible for the progress round, before the 6-month assessment submission deadline, each participant will provide to NIST the progress round package, for final evaluation and judging to make the progress round awards.

5. EVALUATION CRITERIA

DEMONSTRATION ROUND CONTEST

The demonstration round will be evaluated based on the participant's demonstration. The ten unique contests will be evaluated independently to select up to three participants to be awarded prizes for each contest. Up to $650,000 will be awarded, with up to $65,000 per contest. The awards are anticipated to include $30,000 for 1st, $20,000 for 2nd, and $15,000 for 3rd. The awards may vary from contest to contest; in the event of a tie, first and second awards will be combined and split ($25,000 each); or in the event there is a lack of eligible participants, NIST reserves the right to decline to make awards or make fewer awards than anticipated. These awards are made to recognize the technical skill and accomplishments of the participants.

CRITERIA #1: SOLUTION QUALITY (MAX 100/100)

- Does it solve the problem: Level to which the submission demonstrates a solution to the needs of public safety, relevant specifically to the contest's focus and challenge's objectives
- How functional is the solution: Level to which the solution has the potential or actual functionality of a final product capable of being used by the public safety sector
- Quality of the solution: Level to which the participant demonstrates the quality and mastery of their solution as shown by their knowledge of the capabilities and functionality of the software
- Presentation: Skill in presenting the participant's work in a clear and concise presentation, and ability to answer questions live from the judges
- Feasibility and utility design considerations: Including but not limited to size, weight, power, and cost that impact the potential for the solution to be utilized by the public safety sector
- Positive impact: Extent to which solution shows potential for positive impact in the public safety sector

SEED ROUND CONTEST

All participants in the National Award Event Contest are eligible for the seed round. This portion of the contest focuses on business acumen, strategy, and planning. The seed round will be evaluated based on the participant's submission materials, including growth strategy, lean canvas, and other business strategy elements of the participant's submission.

Participants will be evaluated at-large (regardless of contest area) and up to twelve $30,000 prizes are anticipated to be awarded to participants. These twelve participants will also have the opportunity to continue into the progress round.

The number of awards may vary; in the event there is a lack of eligible participants, NIST reserves the right to decline to make awards or make fewer awards than anticipated.

CRITERIA #1: DEVELOPMENT AND SCALABILITY (MAX 20/100)

- Product development: Level to which participant provides a clear path to a functional final product
- Plan for adoption: Likelihood of a transformational product and/or widespread adoption of proposed product or solution
- Differentiation strategy: Extent to which participant identifies other competing products and differentiates proposed product from existing market
- Reality check: Identification of realistic target market(s), discussion of competitive advantage, and the clarity of the business strategy in identifying market objectives (e.g. segment, price, volume/size, and region) and that these objectives are aligned with the participant's capabilities and resources
- Risk mitigation: Identification and accurate assessment of business risks and assumptions

CRITERIA #2: GROWTH STRATEGY (MAX 20/100)

- Quality of the 6-month growth strategy plan including:
    - Success verification methods proposed
    - Indicators of interim progress relevant to product development and market acceptance
    - Risk management
    - Integration participant presentation
    - Realistic approach to completing product development and engaging market segments, and assumptions included within the growth strategy or participant presentation

CRITERIA #3: TEAM POTENTIAL FOR SUCCESS (MAX 20/100)

- Quality and experience of the team
    - Extent to which the training, capabilities, and experience of the assembled team will result in the successful completion of the proposed goals and outcomes.
    - Likelihood that this team will be able to achieve the final outcomes on time and to specification.
    - The team has access to facilities, equipment, and any other resources they would require to complete the proposed outcomes.
- Quality of the partnerships
    - Mentors, Coaches, Investors, and other similar resources
    - Subject matter experts, customers, end users, and other similar resources
- Financial acumen and resources management

PROGRESS ROUND CONTEST

All participants selected in the seed round are eligible for the progress round. This portion of the contest focuses on implementation skill, growth, and progress made by the participants within the six months following the National Award Event. The progress round will be evaluated based on the participant's submission materials, primarily the participant-created scorecard.

Participants will be evaluated by judges to assess their progress against their scorecard metrics and up to ten $70,000 prizes are anticipated to be awarded to participants.

The number of awards may vary; in the event there is a lack of eligible participants, NIST reserves the right to decline to make awards or make fewer awards than anticipated.

CRITERIA: SCORECARD PERFORMANCE

The Judge Panel will evaluate submissions by applicants based on the participant scorecard performance and the extent of progress that has been shown during this 6-month assessment period. Specifically, the judges will evaluate each of the five or more performance metrics provided by each participant in their seed round based on the grading scale of A, B, C, or D as further described below.

Grade A: The participant has exceeded their stated scorecard metric, in a way that has significant positive impact for the public safety sector.

Grade B: The participant has exceeded their stated scorecard metric, in a way that has some positive impact for the public safety sector.

Grade C: The participant has met their stated scorecard metric, with the potential to continue to make progress, towards exceeding the goal. Based on current performance, it is likely that, in the future, the participant will create a significant positive impact for the public safety sector.

Grade D: The level of progress made by the participant does not indicate a likelihood of future success.

In addition to providing a grade for each of the five or more scorecard metrics, the judges will also evaluate each participant's performance on the following two questions with the same grading scale.

Did the participant demonstrate substantial progress to building a viable product or business that has the potential to continue to grow in the public safety sector as outlined in their seed round submission materials?

Did the participants achieve any success in raising outside funding to support their strategy? For example, securing angel investment, venture capital, private equity, or other outside investment?

Across the scorecard metrics and the two required questions, if a participant's average grade is A, the team will receive 100% of the final award. If the average grade is a B, the team will receive 80% of the final award. If the average grade is a C, the team will receive 70% of the final award. If the average grade is a D, then the team will receive no additional funds.

FOR ADDITIONAL INFORMATION

The official rules of the Tech to Protect Challenge can be found on www.challenge.gov with additional information, tools, and data for the challenge at www.techtoprotectchallenge.org.