UAS 3.0 First Responder UAS Triple Challenge: Speed, Resilience, Security

Challenge 3.3: Shields Up! Securing Public Safety UAS Navigation and Control

Introduction

The National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR) announces the ***Shields Up! Securing Public Safety UAS Data Challenge (Shields Up Challenge)***; a 3-stage prize competition that uses your ingenuity and cybersecurity skills to solve threats and vulnerabilities associated with Unmanned Aircraft Systems (UAS). The Challenge seeks skills, ingenuity, expertise, and innovation to improve security on UAS control channels and navigation functions, with prize awards of up to $200,000. You can make a difference! To enter for Stage 1, submit your entry starting August 2, 2021 with a deadline of September 30, 2021. Continue reading to learn more about challenge stages and details. No fees or qualifications are needed to enter the first stage.

Challenge Background

The National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR), in conjunction with Mississippi State University and Kansas State University, is hosting the Shields Up Challenge, with an opportunity to win a final prize of $30,000 in the final stage with total prize awards up to $200,000 for top designs throughout the Shields Up Challenge. PSCR's Open Innovation team engages public safety entities, government, academia, and industry to identify innovation opportunities and foster technology advancements for public safety communications through Prize Competitions and Challenges.

Challenge Goals and Objectives

The purpose of the Shields Up Challenge is to explore and advance the cybersecurity of UAS technology to support first responders in their missions. The use of UAS expands public safety's ability to gather critical data, whether they be from video, cameras, sensors, or peripherals, and allows them to obtain this information more quickly and efficiently than deploying boots-on-the-ground.

Public safety uses a myriad of solutions for their UAS needs, including commercial off-the-shelf (COTS) UAS and open-source/do-it-yourself (DIY) hardware and software. The term UAS applies to many types of aircraft that are being incorporated into public safety missions[1]:

● Crime scene processing ● Cross-agency aid ● Damage assessment (man-made or natural event) ● Disaster response	● Fire or explosives ● Infrastructure inspections ● Major traffic accident investigations	● Search and rescue missions ● Special events or public safety assessments ● Tactical deployment ● Terrorism response

As UAS technology becomes more pervasive in the public safety mission, it will become crucial to protect these assets from disruptions in **navigation** and **control.**

The public safety use case for UAS is multifaceted. However, all UAS must maintain controlled flight and successful navigation at their core in order to complete their missions. A UAS that flies to the wrong location or is delayed in reaching a time-crucial objective is as good as a UAS that has not taken flight. A UAS that is hijacked due to a malicious attacker not only jeopardizes public safety missions, it also compromises responder assets. In both of these cases, the compromised UAS causes **mission failure**.

Contestants in this Challenge are required to frame their threats and countermeasures concerning the disruption and preservation of UAS **navigation and control** to prevent **mission failure**:

- **UAS Navigation -** The ability of the UAS to successfully move between two points within 3D (three dimensional) airspace.
- **UAS Control** - The ability for a pilot-controlled UAS to successfully maintain flight control within a 3D airspace.

With the innovative solutions discovered through this Challenge, PSCR seeks to improve UAS cybersecurity for state and local first responders as they deploy UAS for law enforcement, firefighters, and other emergency services. To accomplish this, we seek to:

- Identify real-world threats to UAS flight, navigation, and control technologies
- Identify countermeasures for these threats
- Demonstrate the threat and countermeasures on a functional UAS.

[1] https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/cops-w0894-pub.pdf

Contestants are required to demonstrate attacks on open-source software for UAS **navigation** and/or **control**. Contestants are encouraged to use innovation and creativity when designing their countermeasures. Possible solutions include but are not limited to:

- Updates and/or modifications to existing open source software
- Newly developed software
- Newly developed hardware
- Secure UAS configuration guidance.

Summary of Challenge Stages

The Shields Up Challenge is a 3-stage competition to design, develop, and demonstrate UAS solutions that improve security on UAS control channels and navigation functions. Below is a summary of each stage of the Challenge.

Stage	Contest Description	Review Criteria Summary	Number of Contestants Eligible to Compete
1	Concept Paper	Strategic Alignment & Technical Outcome; Feasibility & Team	Open to all eligible Contestants
2	Design/Build and Video Evaluation	Check-in Review Team Video Evaluation	Up to 10 Contestants invited from Stage 1
3	Live Demonstration	Auditors Evaluation	Up to 5 Finalists invited from Stage 2

Awards

NIST Public Safety Communications Research program is hosting a 3-stage challenge, with prize awards listed in the following table:

Award Ranking	Number of Awards	Award Value
Stage 1	up to 10	$3,000 each, up to $30,000 total
Stage 2	up to 10	Check-in Review: $2,000 each, up to $20,000 total
Stage 3	up to 5	Live Demonstration: $30,000 each, up to $150,000 total
		Total Challenge Award = $200,000

NOTE: This table only describes prize awards; additional Contestants may win an invitation to participate in challenge stages but not be eligible to receive prize awards. All Stage 3 Contestants are eligible to compete for all Stage 3 prizes.

Key Dates

Date	Event
August 2, 2021	Shields Up Challenge is open for proposal submissions through the challenge website; begin Stage 1
September 30, 2021	Stage 1 Closed for proposal submissions
October 29, 2021	Stage 1 Announce winners; begin Stage 2
December 6 - 10, 2021	Stage 2 Check-In Review conducted with eligible Stage 2 Contestants
December 20, 2021	Stage 2 Check-in - Announce winners
February 21, 2022	Stage 2 Team Video Evaluation conducted with eligible Stage 2 Contestants
March 1, 2022	Stage 2 Team Video Evaluation - Announce winners; begin Stage 3
April 4 - 8, 2022	Stage 3 Live Demonstration Contest will take place at Contestants' designated flight locations while being evaluated by an on-site Challenge auditor
May 1, 2022	Final Winners Announced

Note: NIST reserves the right to revise the dates at any time.

Program Email Address

Questions about the Challenge should be directed to uaschallenge@k-state.edu.

Official Rules

This document outlines the official rules for the ***First Responder UAS Triple Challenge - Shields Up! Securing Public Safety UAS Navigation and Control***. Nothing within this document or in any supporting documents shall be construed as obligating the Department of Commerce, National Institute of Standards and Technology (NIST), or any other Federal agency or instrumentality to any expenditure of appropriated funds, or any obligation or expenditure of funds over or in advance of available appropriations.

SUMMARY OF CHALLENGE

The following is a summary of each contest. For more information, please review the full terms and conditions for each contest as provided throughout this document.

STAGE 1: Concept Paper Contest

The Concept Paper Contest invites all eligible Contestants to complete a concept paper outlining their knowledge, skills, capabilities, and methodology/approach for this Challenge. The concept paper will detail the proposed scenario, attack, and countermeasures and include:

- The challenge area(s) being addressed.
- A detailed scenario that describes the normal functioning of the UAS and how the attack will subvert it.
- A detailed description of the attack.
- A detailed description of the countermeasures.
- A bill of materials (BOM) to be used for the demonstration.

Up to 10 Contestants will receive awards including invitations to advance to Stage 2: Design/Build and Video Evaluation Contest.

STAGE 2: Design/Build and Video Evaluation Contest

In this contest, Contestants will purchase or create the hardware necessary to implement the design approach outlined within their concept paper. Contestants will purchase or create the hardware or parts necessary to build and demonstrate their attack and countermeasures. Contestants will participate in a design review and video evaluation to demonstrate the teams' proposed designs.

- Check-in Review: Up to 10 Contestants will be selected to receive prize awards for submitting documentation required to support the build and design of their countermeasure for submission in the Team Video Evaluation.
- Team Video Evaluation: Contestants will provide videos of live test flights demonstrating their attacks and countermeasures. Contestants will submit a verifiable video of their solution and be ranked. Up to 5 Contestants will receive invitations to Stage 3: Live Demonstration contest based on those rankings.

STAGE 3: Live Demonstration Contest

In this contest, Contestants will demonstrate their countermeasure solution as a live demonstration for an on-site Challenge Auditor at the Contestants designated flight location. These Contestants will have an on-site auditor verify the vulnerability and countermeasure solution, as demonstrated in the video evaluation. Contestants completing at least the minimum standards may receive prize awards.

Safety Specific Requirements:

- All flights shall comply with local, state, and federal laws and regulations.
- All flights shall occur at authorized UAS flying areas.
- All pilots shall be Part 107 certified and covered by UAS insurance with a minimum coverage of $1M before conducting any flights outside of an enclosed test facility.
- All UAS shall be compliant with Part 107 FAA Regulations

Challenge Areas

Contestants in this Challenge are required to frame their threats and countermeasures concerning the disruption and preservation of UAS **navigation and control** within the context of disrupting and preserving the following functions to prevent **mission failure**:

- **UAS Navigation -** The ability of the UAS to successfully move between two points within 3D (three dimensional) airspace.
- **UAS Control** - The ability for a pilot-controlled UAS to successfully maintain flight control within a 3D airspace.

The attack surface for preserving the functions of **navigation** and **control** is extensive. To narrow the scope of this competition, NIST PSCR is interested in threats and countermeasures in UAS open-source software that affects navigation and control in the two areas below:

1. **Protecting the UAS Control Channel** -When operating a UAS, pilots use various radio control channels to direct the UAS. These channels are vulnerable to attack and can be exploited to wrest control away from the pilot.
2. **Protecting UAS Sensory Input (hardware)** - Modern UAS rely heavily on complex sensing, perception, sensor fusion, adaptive control, and auto-calibration systems to maintain stable flight and provide automated navigation functions. Providing inputs that confuse these systems can result in undesirable behavior of the Unmanned Aerial Vehicle (UAV). Such information may be provided through sensors that include, but are not limited to, optical sensors (cameras, LIDAR), radio sensors (RADAR), and inertial sensors (accelerometers, gyroscopes, magnetic compasses). Threats may range from simply overloading the sensors to providing temporal and spatial patterns designed to confuse them.

Challenge Guidance

The Shields Up Challenge is dedicated to technologies concerned with cyber risks, threats, vulnerabilities, impact, and countermeasures for UAS navigation and control systems. However, Contestants will be presented with many design decisions and considerations throughout the course of this challenge. The guidance below is intended to assist Contestants by creating boundaries to design trade-offs and ensure responsible behavior.

- **Open-Source Operating Software.** As part of this Challenge, Contestants must use non-proprietary open-source operating software in their attack target. A wide variety of open-source software projects are supported on pre-built commercial or custom UAS hardware solutions. Contestants are encouraged to explore the most viable options to demonstrate their attack and countermeasure.
- **Interference with Licensed Spectrum and Associated Technologies.** As part of the Challenge, Contestants must comply with all laws and guidelines associated with federally and/or commercially licensed spectrum. This includes, but is not limited to, global positioning system (GPS)[2], long term evolution (LTE), and automatic dependent surveillance broadcast (ADS-B) frequencies. As part of the Challenge, Contestants shall not manufacture or operate any device that interferes with these frequencies/technologies. If Contestants choose to demonstrate weakness or vulnerabilities with these technologies, they must simulate the effects of the interference so as not to actively interfere with the normal operation of these technologies.
- **Vulnerability Disclosure.** If an unknown exploitable vulnerability in a commercial UAS is discovered in the process of a Contestant building an attack or countermeasure, it is both ethical and responsible for NIST and the Contestant to disclose in good faith that vulnerability to the UAS manufacturer. The UAS manufacturer is then able to take appropriate actions to minimize harm and liability.

Disqualifying Solutions

The following areas are grounds for disqualification:

- **Law and Regulations.** Failure to comply with any law and/or regulation regarding UAS operation will result in disqualification.
- **Proprietary or Commercial off-the-shelf (COTS) Software**. Proprietary software may be used during the operation of the attack target, however, this software may not be the subject of the attack. At this time, this Challenge will not permit the testing of COTS software. However, should NIST receive permission from one or more commercial UAS manufacturers to include their UAS or COTS as part of the competition, NIST may update the rules of the competition to permit use of one or more specific manufacturers' commercial or proprietary software. Contestants must not use

[2] FCC *Alert Jammer Enforcement* (FCC, 2020)

commercial or proprietary software as part of the Challenge absent specific NIST permission to do so.

- **Non-Cybersecurity Solutions.** The Challenge is looking to support innovative technologies related to cybersecurity but will disqualify specific technical solutions that do not, at their core, embrace the cybersecurity countermeasures. Solutions that involve either the attack or countermeasure causing physical damage or destruction of the target UAS will be disqualified.
- **Simple Jamming Attacks**. Be aware that Federal law prohibits the operation, marketing, or sale of any type of jamming equipment that interferes with authorized radio communications, including cellular and Personal Communication Services (PCS), police radar, and Global Positioning Systems (GPS). A Contestant's attack scenario cannot rely on simply jamming the control channel of the target. Any Attack scenarios of which jamming is a component of a greater attack are permissible if the jamming is simulated and no jamming equipment is employed.

STAGE 1: Concept Paper

The Concept Paper Contest invites all eligible Contestants to complete a concept paper outlining their knowledge, skills, capabilities, and approach for this Challenge. Contestants' concept papers will be reviewed by a panel of subject matter experts and judges who will make their selections based on the clarity and feasibility of the submission. Contestants selected by the Judging panel will be eligible to move forward to Stage 2: Design/Build, and Video Evaluation Contest. All eligible Contestants are encouraged to submit completed concept papers for review.

How to Enter:

Visit the Challenge website [https://www.uastriplechallenge.com] to review the challenge stages in the Shields Up Challenge.

- Visit Challenge.gov to review the series of contests in the Shields Up Challenge.
- Contestants will review the terms and conditions of participation and accept the terms and conditions for entry.
- Complete the Concept Paper Contest submission requirements and submit the required concept paper and summary templates via the Challenge website [https://www.uastriplechallenge.com].

Concept Paper Content Requirements:

The concept paper shall be created and submitted by all registered users on the Shields Up Challenge website [https://www.uastriplechallenge.com]. The concept paper must contain the following 6 sections:

1. The Cover Page and Abstract
2. Mission Scenario

3. Attack Description
4. Countermeasure Description
5. Project Roadmap
6. Threat Demonstration Plan
7. Bill of Materials

Section 1:	Cover Page and Abstract	**Word/Page Limit:**	1 page
Description and Contents			
The cover page must include the following items: ● Team name ● The names of all individuals associated with the team ● Chosen **Challenge Area(s)** ● Abstract (500 words) - a brief description of the attack scenario and the countermeasure proposed by the team			

Section 2:	Mission Scenario	**Word/Page Limit:**	500 words
Description			
This section must detail a UAS public safety mission and how the proposed threat causes a complete mission failure. That is, the Contestant must describe how the **threat** will affect the control system in a way that significantly disrupts the **navigation** and/or **control** of the UAS. The purpose of this section is to establish that the Contestant has a sufficient understanding of public safety missions and that the proposed disruption represents a real and actual threat to public safety. Furthermore, it will give Contestants the opportunity to clearly define and justify what **mission failure** looks like in the context of their selected mission scenario. Finally, it will also inform the efficacy of the demonstration detailed in **Section 6.** At a minimum, the scenario must include: ● Description of the mission goals ● Mission setting ● Mission failure parameters and justification ● Attack consequences			

Section 3:	Attack Description	**Word/Page Limit:**	1000 words

Description

This section must detail the attack against the UAS. Contestants must describe the attack process, parameters, and requirements and how they interface with the chosen **Challenge Area(s)**. Furthermore, they must identify any vulnerabilities being leveraged as part of the attack. This section must contain enough detail for judges to evaluate the feasibility and practicality of the attack scenario.

At minimum, this section should include:

- Attack Vector - What technology(ies) the Contestant means to exploit
- System Impact - How the attack affects the UAS and its ability to **navigate** and/or be **controlled**
- Build parameters -- How the Contestant plans to build the attack for demonstration
    - Hardware requirements
    - Software requirements
    - Broadcast parameters * (if applicable)
- How the attack relates to the mission failure described in **Section 2**

*The Contestants are required to follow all federal, state, and local laws governing radio broadcast.

Section 4:	Countermeasure Description	**Word/Page Limit:**	500 words

Description

This section must detail the proposed countermeasure(s). The form of the countermeasure(s) is primarily up to the Contestant. It can take the form of either preventive or reactive measures. This section should provide enough detail about the countermeasure(s) so as to be clear of its intended operation. Countermeasures can include, but are not limited to:

- Modifications to existing UAS software including configuration parameters
- Wholly new hardware or software components
- Protocol modification
- New or modified system behavior, including automated actions and feedback loops.

Section 5:	Project Roadmap	**Word/Page Limit:**	1000 words

Description

This section must contain a detailed plan for how the Contestant will transition from their concept paper to their attack and countermeasure builds. The plan should identify

intermediary research, milestones, and build activities for both Stages 2 and 3 of this competition. It should also include estimated completion dates for each such objective.

Section 6:	Threat Demonstration Plan	**Word/Page Limit:**	1000 words
Description			
Later stages in this contest will require that Contestants provide video demonstrations of their attacks and countermeasures. This section should describe how the Contestant will convey these via the required format. Contestants should describe how their filmed examples map into the scenario they detailed in Section 1. They should discuss how they will visually depict the mission failure (i.e. the attack). Furthermore, they should detail any safety precautions they will take. Finally, they should show how the demonstration will fulfill any legal requirements. A video demonstration must be repeatable and is encouraged to be specific in execution so that no technology is in question. For example, if an attack is broadcasting a signal via WiFi, all possible efforts must be taken to show that a behind-the-scenes actor is not manipulating input. The same must be valid for all countermeasures.			

Section 7:	Bill of Materials	**Word/Page Limit:**	1 page
Description			
This section must include a detailed list of the materials that Contestants will use. It must consist of all hardware and software components used to demonstrate the attack and those used in any proposed countermeasures. It must also list the maximum gross takeoff weight (MGTW). An updated BOM is required in Stage 2.			

NOTE: Submission(s) must not use NIST's logo or official seal and must not claim NIST endorsement.

Evaluation Criteria and Judging:

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

Stage 1 Scoring Criteria:

Criteria Title	Criteria Definition	Criteria Requirement
Completeness (Pass/Fail)	Completeness of the document is defined by how well the document answers the question and requirements of the challenge.	The document must contain all sections and required information specified above in the Concept Paper Content Requirements section.
Understandability (40%)	Understandability of the document is defined by how well the audience of the document is able to describe the details, regardless of the amount of technical information within the document.	The document must be easily understood from both a layman's point of view and a judge's point of view. It must detail both the attack scenario and countermeasures in a manner that fully supports how the Contestant will achieve success in subsequent stages.
Feasibility (60%)	Feasibility is defined by how realistic, and in scope, the solution is with a high likelihood of meeting the requirements.	The document must showcase the feasibility of the solution in full detail. It must describe the robustness, repeatability, and sustainability of the proposed solutions and detail a sufficient Project Roadmap and Demonstration Plan. Solutions that are deemed to be impossible, impractical or inadequate may be eliminated.

Concept Papers will be evaluated based on the Scoring Criteria above. The specific scores will not be released publicly or provided to the Contestant. Up to 10 Contestants will be awarded prize awards of $3,000 each and receive an invitation to Stage 2: Design/Build and Video Evaluation.

STAGE 2: Design/Build and Video Evaluation

In this stage, Contestants will implement the design approach from their concept paper by building their UAS prototype solution, submitting materials for Check-in Review and submitting a video for the Team Video Evaluation. Contestants will purchase or create (for example: using 3D printing or machining) the hardware or parts necessary to build and demonstrate their attack and countermeasures. Contestants will participate in a design review to demonstrate progress and a video evaluation to prove the teams' proposed design. Contestants selected by the Judging panel as winners in the Check-in Review may receive prize awards and/or may win invitations to participate in the Team Video Evaluation. Winners of the Team Video Evaluation will win invitations to Stage 3.

How To Enter Stage 2:

Visit the Challenge website [https://www.uastriplechallenge.com] to review the stages in the Shields Up Challenge.

- Once Contestants are selected from Stage 1, they will be required to participate in a Stage 2 challenge webinar.
- Contestants will review the terms and conditions of participation and accept the terms and conditions for entry.
- Contestants will be required to participate in a Check-in Review meeting.
- Eligible Contestants, who won an invitation from the Check-in Review, will submit a UAS flight video demonstrating their countermeasure solution for review and evaluation.

Check-in Review Requirements:

The Check-in Review is a meeting between the NIST Challenge team and Contestants to demonstrate their progress toward achieving their proposed design. During the Check-in Review, Contestants will present information about their progress towards a functional demonstration of a system attack and countermeasure. Contestants will present details of the planned design, estimated or actual BOM, an actual implemented subsystem, and a status of the project schedule.

For the Check-in Review, do not include proprietary or sensitive information. The check-in meeting will be scheduled for all eligible Contestants using an online form available through [https://www.uastriplechallenge.com]. Check-in Review will be judged and scored based on the review documents and presentation with content that shall include the following:

Section	Page Limit	Description
Cover Page	1 Slide	Includes: • Contestant Name(s) • Application Title • Technical/Business points of contact
Project Description	10 Slides	• Description of successful mission parameters • Explanation of mission disruption • Technical details regarding attack implementation • Explanation of proposed countermeasure • Current system design plans/schematics
Project Schedule	1 Slide	The project schedule should include milestone dates through the end of Stage 3 as derived from Project Roadmap of the Concept Paper.
UAS Bill of Materials	1 Slide	Single summary slide for separate BOM that reflects the cost of the entire design including countermeasure system.

Attack Bill of Materials	1 Slide	Single summary slide for separate BOM that details materials required to implement an attack on a UAS control system.

Bill of Materials (BOM) Requirements:

Contestants must keep records of all hardware and software purchased or created for the prototype to function and ensure compliance in the Challenge. The BOM shall include:

- Each item in the system with its part number, internet link or URL that identifies where to procure the item, unit cost, quantity, and total cost.
- Custom made items shall have the unit cost estimated, their fabrication source defined, material, and material volume estimated.
- All open source software and their associated licenses.

Video Evaluation Requirements:

The format and content of the video is left largely to the Contestants. However, the video shall clearly depict two major scenes: 1) how the attack leads to a complete failure of mission, and 2) that the countermeasure thwarts the effects of the attack. Contestants should reasonably show that these two scenes are happening in real time and are not fabricated or simulated. Cybersecurity activities and their internal effects are often difficult to demonstrate visually. Therefore, props, stand-ins, and visual aides are permitted in the video to clarify to the viewer the subject being depicted.

The video shall have the following characteristics:

- A successful, completed mission with no active attack or countermeasure system.
- A failed mission with an active attack but no countermeasure system.
- A completed mission with both an active attack and countermeasure system.
- A ‘tour’ of the attack system:
    - Walkthrough all major components
    - Details of its operating environment
- A ‘tour’ of the countermeasure system:
    - Walkthrough all major components
    - Operating parameters
- Is no less than 1280 x 720 resolution
- Is no more than 30 minutes in length

Evaluation Criteria and Judging

NIST will review the Check-in Review materials and Team Video Evaluation submission for all eligible Stage 2 Contestants. A submission that fails to meet the compliance criteria for Check-in Review may be disqualified from the Challenge or may be invited to submit a video for the

Team Video Evaluation and not receive prize awards. Submissions will be evaluated and scored by a panel of judges. An evaluation of a submission by a panel of judges does not constitute NIST's final determination of contestant or submission eligibility. Submissions will be judged according to the criteria below:

Stage 2 Check-in Review Scoring Criteria:

Criteria Title	Criteria Definition	Criteria Requirement
Completeness (Pass/Fail)	Completeness of the Check-in Review is defined by how well the materials presented address the details of the planned system design.	The review must sufficiently outline the Status of the proposed attack and countermeasure. Documents, slides, or presentation materials shall be submitted for review.
Project logistics (30%)	Project logistics of the Check-in Review is defined by how well the materials presented address the overall planning of the project.	The review must sufficiently outline the status of ordered parts, components, or subsystems and provide a BOM. The review must accurately detail the status of the Project Roadmap. Contestants may include revisions/adjustments made to the roadmap up to this point.
Feasibility (70%)	Feasibility is defined by how realistic, and in scope, the solution is with a high likelihood of meeting the requirements.	The Contestant must showcase the feasibility of the solution in full detail and demonstrate sufficient progress towards project goals. Contestants will present information about their design and progress towards a functional demonstration of an attack and countermeasure. Contestants may present design plans, prototype solutions, or partial/in-progress builds.

Stage 2 Team Video Evaluation Scoring Criteria:

Criteria Title/Weight	Criteria Definition	Criteria Requirement
Completeness (Pass/Fail)	How well the video answers the requirements of the challenge.	Video must include everything previously outlined in the Video Evaluation Requirements.
Scenario Alignment (30%)	How well the video demonstration relates to, and represents, the scenario described in the concept paper.	The video must depict the attacks and countermeasures in a setting (or suitable setting facsimile) that corresponds with the scenario and mission failure.[3]
Demonstration Effectiveness (30%)	How well the video conveys the attack and countermeasures	The video must clearly show how each of the substantive steps in the attack and countermeasure demonstrations functions.
Validity of Solution (20%)	How effective the proposed countermeasures are for public safety	The attacks and countermeasures depicted in the video should align with both the solutions depicted in the Check-in Review as well as the how well they align with the needs of public safety.
Composition (20%)	The composition of the video is defined by how well the video is edited and flows throughout the presentation. Video must have a clear and concise composition that does not distract the viewer from the details being shown in the video.	The composition of the video is defined by how well the video is edited and flows throughout the presentation. Video must have a clear and concise composition that does not distract the viewer from the details being shown in the video.

Check-in Reviews and Team Video Evaluations will be evaluated based on the Scoring Criteria in the tables above. The specific scores will not be released publicly or provided to the Contestant. Up to 10 Stage 2: Check-in Review Contestants will be selected to receive prize awards of $2,000 each and an invitation to advance to Stage 2: Team Video Evaluation. Contestants who did not win a prize award may still win an invitation to advance to the Stage 2: Team Video Evaluation.

[3] This is not to mean that scenarios have to be created in perfect 1:1 detail with a real public safety scenario. For example, if the Contestant describes the attack and mission failure during a forest fire scenario, the Contestant need not stage a forest fire in their video. Rather, the operation of the UAS during the demonstration must have a clear mapping into the activities undertaken during a forest fire scenario.

Up to 5 Stage 2: Team Video Evaluation Contestants will win an invitation to advance to Stage 3: Live Demonstration.

STAGE 3: Live Demonstration

Stage 3 is the final stage of the challenge and consists of an in-person demonstration and evaluation at the Contestants' location by a challenge representative. All Contestants will be required to complete a UAS safety check prior to flights.

How To Enter Stage 3:

Visit the Challenge website [https://www.uastriplechallenge.com] to review the stages in the Shields Up Challenge.

- Stage 2 winners should be prepared to complete a UAS safety check prior to flights for the live, in-person demonstration.
- Once Contestants are selected from Stage 2, they will be required to participate in an introduction and Stage 3 challenge webinar.
- Contestants will undergo safety inspections and verification of FAA and FCC compliance immediately prior to the live demonstration.
- Contestants will pilot their UAS to demonstrate the attack/countermeasure solution.
- Contestants will designate the flight location for the live demonstration and challenge staff will make travel arrangements for the on-site Challenge Auditor.

Live Demonstration Requirements:

The live demonstration flights shall be done in a safe manner and follow all the requirements outlined below for the Demonstration, Flight and Weather requirements.

Demonstration Requirements:

The live demonstration will take place at the Contestants' designated flight location with an on-site Challenge Auditor present. Contestants will re-enact the UAS flights submitted for the Stage 2: Team Evaluation. Prior to each flight, a UAS safety check will be performed to ensure FAA compliance. An inspection by the Challenge Auditor will identify and confirm the UAS parts and components that were used to support the attack/countermeasure solution are included in the Stage 2 BOM submission. A complete checklist of items to be inspected and audited will be provided to the Contestant prior to the date of the live demonstration.

Contestants will pilot their UAS to demonstrate:

- A successful, completed mission with no active attack or countermeasure system.
- A failed mission with an active attack but no countermeasure system.
- A completed mission with both an active attack and countermeasure system.

Flight Requirements:

Prior to flying, teams will be required to submit a flight log detailing a minimum of 10 piloted flight hours. The flight log should, at a minimum, detail the number of flights, and duration of

each flight. To ensure safety and compliance with Part 107 FAA regulations throughout the duration of the flight, teams must adhere to the flight requirements outlined below. Failure to adhere to the flight requirements may result in disqualification from Stage 3.

- All operators or pilots must be Part 107 FAA certified or under the supervision of a certified pilot who is a member of the team.
- All operators or pilots must ensure visual line of sight of the UAS as described by Part 107 rules, at all times.
- All operators or pilots must ensure that the UAS maintains an altitude of 400ft AGL (above ground level) or less.
- All operators or pilots must ensure that the UAS remains within the designated search area bounds.

Weather Requirements:

Due to practical restraints and safety considerations, Contestants may request the in-person demonstration to be rescheduled based on safe performance of the UAS flight in Stage 3. Similarly, the on-site auditor may request a delay or reschedule of the Contestant flight due to severe weather or other local concerns.

Evaluation Criteria and Judging:

NIST will review on-site auditor results for each Contestant's live UAS flights. A demonstration that fails to meet the compliance criteria will be disqualified. Demonstrations that pass the initial compliance review will be evaluated and scored by a panel of judges. An evaluation of a demonstration by a panel of judges does not constitute NIST's final determination of contestant or demonstration eligibility. Demonstration will be judged according to the criteria below:

Stage 3 Live Demonstration Scoring Criteria:

Criteria	Criteria Definition	Criteria Metric
UAS Safety Review	Reviews the UAS safety redundancies and capabilities in compliance with FAA Part 107 Regulations.	Pass/Fail
Live Demonstration Results	Contestants will demonstrate 1) a successful, completed mission with no active attack or countermeasure system, 2) a failed mission with an active attack but no countermeasure system, 3) a completed mission with both an active attack and countermeasure system.	Pass/Fail

	All demonstrations will be subject to inspection if interfering inputs are not verifiable.	
UAS/System Inspection	Contestants will complete the Auditor checklist to verify consistency with Stage 2 submission. An inspection by the Auditor of UAS components for the solution must match the Stage 2 BOM.	Pass/Fail

Demonstrations in Stage 3 will be evaluated based on the Scoring Criteria in the table above. The specific scores will not be released publicly or provided to the Contestant.

Final Prize Award Evaluation:

For the five Finalist awards, Contestants will be evaluated using a pass/fail scoring system. Contestants who pass Stage 3 Scoring Criteria may receive a Finalist award of $30,000.

NIST reserves the right to decline to make awards or make fewer awards than anticipated.

Terms and Conditions

Terms and Conditions for Submission Requirements:

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

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

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

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

No Endorsement:

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

Judging Panel:

The submissions will be judged by a qualified panel of expert(s) selected by the Director of NIST. The panel consists of Department of Commerce, National Institute of Standards and Technology and non-Department of Commerce, National Institute of Standards and Technology experts who will judge the submissions using the judging criteria identified above in order to select winners. Judges will not (A) have personal or financial interests in, or be an employee, officer, director, or agent of any entity that is a registered Contestant in a challenge; or (B) have a familial or financial relationship with an individual who is a registered Contestant.

The decisions of the Judging panel for the challenge will be announced in accordance with the dates noted in the "Important Dates" section of these rules. NIST PSCR will not make Contestants' evaluation results from the Judging panel available to Contestants or the public.

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

Verification of Potential Winners:

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

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

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

Winners Not Eligible for Cash Prizes:

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

Eligibility Requirements:

A Contestant (whether an individual, private entity, or team ("Contestant" herin)) must have registered to participate and complied with all of the requirements under Section 105 of the America COMPETES Reauthorization Act of 2010 (Pub. L. No. 111-358), as amended by Section 401 of the American Innovation and Competitiveness Act of 2016 (Pub. L. No. 114-329) and codified in 15 U.S.C. §3719 (hereinafter "America COMPETES Act" or "15 U.S.C. §3719) as contained herein.

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

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

- Individual: a person age 18 or older at time of entry and a U.S. citizen or permanent resident of the United States or its territories.
- Private Entity: a company, institution, or other organization that is incorporated in and maintains a primary place of business in the United States or its territories.
- Team: a group of individuals or a group of private entities, with at least one member of the team meeting the definition for either Individual or Private Entity.
- Contestants not eligible for cash prizes: a contestant that enters the challenge without the ability to claim a cash prize based on the eligibility requirements above. Contestants not eligible for cash prizes must be 18 years or older at time of entry and cannot be

individuals on the denied persons list nor from entities or countries sanctioned by the United States Government.

For all Contestants, general eligibility requirements include:

- Contestants may not be a Federal entity or Federal employee acting within the scope of their employment.
- Contestants may not be a NIST employee.
- Non-NIST Federal employees acting in their personal capacities should consult with their respective agency ethics officials to determine whether their participation in this Challenge is permissible. A contestant shall not be deemed ineligible because the individual or entity used Federal facilities or consulted with Federal employees during this challenge if the Federal employees and facilities are made available to all contestants on an equitable basis.
- Contestants may not be a NIST contractor or associate, or private entity providing services to NIST acting within the scope of their contract, employment, or funding or acquisition agreement with NIST which would involve the use of NIST funding to support a contestant's participation in the challenge.
- Contestants may not be individuals or private entities which provide program support services to NIST including strategic planning, project / program management, communications, reporting, program evaluation, or other similar services to NIST.
- Individuals who are former NIST Federal Employees or NIST Associates are not eligible to enter as an individual or member of a team for 365 days from their last date of paid employment or association with NIST with the exception of individuals in a student internship, experiential learning, or similar temporary employment status.
- Any individuals (including an individual's parent, spouse, or child) or private entities involved with the design, production, execution, distribution or evaluation of the Challenge are not eligible to enter as an individual or member of a team.
- Employees of any official co-sponsoring entities are not eligible to enter.
- A Contestant (whether participating as an individual, private entity, or member of a team) must not have been convicted of a felony criminal violation under any Federal law within the preceding 24 months and must not have any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.
- Contestants must not be suspended, debarred, or otherwise excluded from doing business with the Federal Government.
- Individuals currently receiving NIST funding through a grant or cooperative agreement are eligible to compete but may not utilize the NIST funding for competing in this challenge.
- Previous and current PSCR prize challenge contestants are eligible to enter.

All Contestants must designate an Official Representative:

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

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

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

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

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

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

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

Submission Rights:

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

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

Warranties:

Each Contestant represents and warrants that the Contestant is the sole author and copyright owner of the submission; that the submission is an original work of the Contestant and that the

Contestant has acquired sufficient rights to use and to authorize others, including the Department of Commerce, National Institute of Standards and Technology, to use the submission, as specified throughout the Official Rules, that the submission does not infringe upon any copyright or upon any other third party rights of which the Contestant is aware; and that the submission is free of malware.

The Contestant represents and warrants that all information submitted is true and complete to the best of the Contestant's knowledge, that the Contestant has the right and authority to submit the entry on the Contestant's own behalf or on behalf of the persons and entities that the Contestant specifies within the entry, and that the entry (both the information and materials submitted in the entry and the underlying technology/method/idea/treatment protocol/solution described in the entry):

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

No Confidential Information:

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

Additional Terms and Conditions:

This document outlines the Official Rules for the *First Responder UAS Triple: Shields Up Challenge*. Nothing within this document or in any documents supporting the *First Responder*

UAS Triple: Shields Up Challenge shall be construed as obligating the Department of Commerce, NIST or any other Federal agency or instrumentality to any expenditure of appropriated funds, or any obligation or expenditure of funds in excess of or in advance of available appropriations.

Challenge Subject to Applicable Law:

All challenge phases are subject to all applicable federal laws and regulations. Participation constitutes each Contestant's full and unconditional agreement to these Official Rules and administrative decisions, which are final and binding in all matters related to the challenge. Eligibility for a prize award is contingent upon fulfilling all requirements set forth herein. This notice is not an obligation of funds; the final award of prizes is contingent upon the availability of appropriations.

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

Resolution of Disputes:

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

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

Publicity:

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

Except where prohibited, participation in the Challenge constitutes each winner's consent to the Department of Commerce, National Institute of Standards and Technology's, its agents', and any Challenge Co-Sponsors' use of each winner's name, likeness, photograph, voice,

opinions, and/or hometown and state information for promotional purposes through any form of media, worldwide, without further permission, payment or consideration.

Payments:

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

All cash prizes 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.

Liability and Insurance:

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

Contestants are required to demonstrate UAS (liability) insurance or demonstrate financial responsibility with a minimum coverage of $1M prior to conducting any flights outside of an enclosed test facility for claims by a third party for death, bodily injury, or property damage, or loss resulting from an activity carried out in connection with participation in this Challenge and for claims by the Federal Government for damage or loss to Government property resulting from such an activity. The Federal Government shall be named as an additional insured under the contestant's insurance policy. Contestants are required to maintain such UAS (liability) insurance for the duration of Stages 2 and 3 of the Challenge. Depending on the site for Stage 3 of the Challenge, the flight-testing facility may also be required, named additional insured under the contestant's insurance policy.

Records Retention and FOIA:

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

508 Compliance:

Contestants should keep in mind that the Department of Commerce, National Institute of Standards and Technology considers universal accessibility to information a priority for all individuals, including individuals with disabilities. The Department is strongly committed to meeting its compliance obligations under Section 508 of the Rehabilitation Act of 1973, as amended, to ensure the accessibility of its programs and activities to individuals with disabilities. This obligation includes acquiring accessible electronic and information technology. When evaluating submissions for this challenge, the extent to which a submission complies with the requirements for accessible technology required by Section 508 will be considered.

General Conditions:

This prize competition shall be performed in accordance with the America COMPETES Act.

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

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

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