December 7, 2016

NOTICE OF FUNDING OPPORTUNITY (NOFO)
NIST Public Safety Innovation Accelerator Program (PSIAP)

EXECUTIVE SUMMARY

- **Federal Agency Name:** National Institute of Standards and Technology (NIST), United States Department of Commerce (DoC)

- **Funding Opportunity Title:** NIST Public Safety Innovation Accelerator Program

- **Announcement Type:** Initial

- **Funding Opportunity Number**: 2017-NIST-PSIAP-01

- **Catalog of Federal Domestic Assistance (CFDA) Number:** 11.609, Measurement and Engineering Research and Standards

- **Dates:** Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, Tuesday, February 28, 2017. Applications received after this deadline will not be reviewed or considered. **Applicants should be aware, and factor in their application submission planning, that the Grants.gov system is expected to be closed for routine maintenance from 12:01 Eastern Time, Saturday, December 17, 2016 until Monday, December 19, 2016 at 6:00 a.m. Eastern Time, and also from 12:01 Eastern Time, Saturday, January 21, 2017 until Monday, January 23, 2017 at 6:00 a.m. Eastern Time, and again from 12:01 Eastern Time, Saturday, February 18, 2017 until Tuesday, February 21, 2017 at 6:00 a.m. Eastern Time.** Applications cannot be submitted when Grants.gov is closed. NIST expects to complete its review, selection of successful applicants, and award processing by May 2017. NIST expects the earliest start date for awards under this NOFO to be June 1, 2017.

  Applicants are strongly urged to read Section IV.2.b. Attachment of Required Application Documents found on page 29 of this NOFO with great attention. Applicants should carefully follow the instructions and recommendations regarding attachments and use the Download Submitted Applications feature on www.grants.gov to check that all required attachments were contained in their submission. Applications submitted without the required documents will not pass the Initial Administrative Review, described in Section V.3.a. of this NOFO.

  When developing the submission timeline, please keep in mind that: (1) all applicants are required to have a current registration in the electronic System for Award Management (SAM.gov); (2) the free annual registration process in the SAM.gov (*see* Section IV.3 and Section IV.7.a.(1).b of this NOFO) often takes

between three and five business days and may take as long as two weeks; (3) electronic applicants are required to have a current registration in Grants.gov; and (4) applicants using Grants.gov will receive email notifications over a period of up to two business days as the application moves through intermediate systems before the applicant learns via a validation or rejection notification whether NIST has received the application. (See www.grants.gov for full information on application and notification through Grants.gov). Please note that a federal assistance award cannot be issued if the designated recipient's registration in the System for Award Management (SAM.gov) is not current at the time of the award.

- **Application Submission Address:** Applications must be submitted using Grants.gov.

- **Funding Opportunity Description:** The NIST Public Safety Innovation Accelerator Program seeks applications from eligible applicants for activities to accelerate research, development, production, and testing of key broadband technologies and capabilities for first responders as described in Section I. of this NOFO.

- **Anticipated Amounts:** In FY 2017 through FY2019, NIST anticipates up to $30,000,000 may be available to fund awards in the range of $10,000 to $1,000,000 per year with project performance periods of up to two (2) years. Proposals submitted by institutions of higher education with the specific purpose of supporting research by students as part of their doctoral program may have performance periods of up to three (3) years. All awards will be made consistent with the multi-year funding policy (*see* Section II.2 of this NOFO).

- **Funding Instrument:** Grant or cooperative agreement, as appropriate.

- **Eligibility:** All awards listed in this NOFO are open to all non-Federal entities. Eligible applicants include institutions of higher education, non-profit organizations, for-profit organizations, state and local governments, Indian tribes, hospitals, foreign public entities, and foreign governments. An eligible organization may propose to work individually or to include proposed sub-awardees, contractors or other collaborators. Please note that individuals and unincorporated sole proprietors are not considered "non-Federal entities" and are not eligible apply under this NOFO.

  NIST will only consider one application per applicant; however, an applicant entity may be proposed as a sub-recipient, contractor, or unfunded collaborator within applications submitted by other entities. In addition, an applicant may address more than one technology area from the program description, though they should make this very clear in the technical proposal.

- **Cost Sharing Requirements:** Matching funds are not required for this NOFO.

- **Public Website, Frequently Asked Questions (FAQs) and Webinar:** NIST has a public website (www.nist.gov/ctl/pscr or www.pscr.gov) that provides information pertaining to this Funding Opportunity[1]. NIST anticipates that a "Frequently Asked Questions" section or other resource materials will be maintained and updated on the website as needed to provide additional guidance and clarifying information that may arise related to this Funding Opportunity. Any amendments to this NOFO will be announced through Grants.gov.

  Applicants must submit all questions pertaining to this funding opportunity in writing to pscr@nist.gov. Questions submitted to NIST may be posted on www.nist.gov/ctl/pscr. Alternatively, applicants may ask questions during the informational public webinar as described in the next paragraph.

  NIST will host a webinar to provide general information regarding this NOFO, offer general guidance on preparing applications, and answer questions. Scheduling details about the webinar will be available at www.nist.gov/ctl/pscr. Proprietary technical discussions about specific project ideas will not be permitted and NIST staff will not critique or provide feedback on specific project ideas while they are being developed by an applicant or brought forth during the webinar or at any time before the deadline for all applications. However, questions about the PSIAP, eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application can be addressed at the webinar and by e-mail to pscr@nist.gov as described in the previous paragraph. There is no cost to attend the webinar, but participants must register in advance. Participation in the webinar is not required, and will not be considered in the application review and selection process. Additional information on the PSIAP and webinar is available at www.nist.gov/ctl/pscr.

Table of Contents

[1] Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Programmatic and Technical Questions, if this link is no longer working or more information is needed.

FULL ANNOUNCEMENT TEXT

I. Program Description

The statutory authority for the NIST Public Safety Innovation Accelerator Program is 15 U.S.C. § 272(b)(4) and 47 U.S.C. § 1443.

The NIST Public Safety Innovation Accelerator Program (PSIAP) is seeking applications to accelerate research, development, production, and testing activities in six specific technology areas: mission critical voice; location based services (LBS); public safety analytics; communication demand modeling; research and prototyping platforms; and resilient systems. The PSIAP is one of several initiatives within the NIST Public Safety Communications Research (PSCR) program. More information about the PSCR, as well as technology roadmaps and summit reports for LBS and public safety analytics, can be found at www.nist.gov/ctl/pscr.

The PSIAP was established in support of the emerging Nationwide Public Safety Broadband Network and in recognition of the urgent need for first responders to have access to the same broadband communications and innovative technologies that consumers on commercial networks now expect. Each of the six technology areas, described in more detail in Sections I.A. through I.F. of this NOFO, include specific objectives prioritized by public safety stakeholders, ranging from the migration of current capabilities to broadband networks, e.g., mission critical voice, to the development of emerging technologies, e.g., analytics, that could transform the future of public safety operations.

Recipients will rapidly accelerate the objectives of the PSIAP through innovative research and development (R&D) projects. Applicants may propose projects specific to one or multiple PSIAP technology areas and may propose cross-cutting projects that address one or more objectives within each or multiple technology areas. Applicants may also propose new ideas and objectives within any of the technology areas, but may not propose new technology areas.

Where appropriate, applicants should propose projects that include active and sustained engagement with first responders. This to ensure that the R&D outputs of each PSIAP project are highly relevant and will have a meaningful impact on the public safety community. The PSIAP recognizes that operational demands and limited budgets typically preclude public safety entities from dedicating resources to participate in R&D activities. Therefore, applicants are encouraged to identify appropriate partners and include funding in their proposed budget for non-federal first responders and public safety personnel to actively participate within their projects, and to budget significant time and sufficient travel for this interaction. Please note that Federal entities are not eligible to receive funding under this NOFO, though they may participate as unfunded collaborators. Researchers who are proposing work that would benefit from the

involvement of public safety personnel, but who have not identified suitable partners, are nevertheless encouraged to apply.

Applicants should also plan R&D projects tailored to disseminate their ideas and technology to the public safety stakeholder community. Such activities may be achieved through publications, technology transfer, including commercialization, training, or the release of tools, designs, and/or data sets. Applicants may include funding in their proposed budget that would support the dissemination of the results and lessons of their PSIAP R&D efforts to the public safety stakeholder community.

For applications specific to Public Safety Analytics (*see* Section I.C of this NOFO), letters of commitment from the public safety community are required (*see* Section IV.2.a.(9) of this NOFO) and will be considered during the evaluation of Technology Area 3 technical proposals (*see* Section V.1.c and V.1.e of this NOFO). For purposes of this NOFO, public safety includes U.S. federal, state, and local emergency medical services, fire services, and law enforcement. For applications specific to Technology Areas other than 3, letters of commitment from the public safety community are encouraged, but not required.

In order to facilitate impactful partnerships between industry and public safety, PSCR will maintain a list of public safety organizations (PSOs) that have expressed interest in participating in the PSIAP. Interested PSOs should send an e-mail to pscr@nist.gov expressing their interest along with their specific areas of expertise or concern, and points of contact. Potential applicants may request information about interested PSOs by sending an e-mail to pscr@nist.gov. Note that partnerships are not limited to only those PSOs and applicants who have submitted or requested information, i.e. any applicant can partner with any PSO, subject to the eligibility requirements in this NOFO. Applicants are encouraged to develop partnerships with PSOs on their own. Potential applicants are responsible for contacting the organizations and arranging partnerships. NIST will not assist potential applicants with finding partners.

A. Mission Critical Voice

Ever increasing operational demands on first responders, along with new technological opportunities and capabilities, are driving PSOs to adopt broadband technologies such as Long Term Evolution (LTE) for mission critical data. While access to broadband data is improving public safety operations and providing new applications, voice remains the most critical communications capability. However, a true mission critical voice (MCV) capability has yet to be deployed on any LTE network. The PSIAP is seeking proposals for innovative R&D projects to accelerate the development, production, and testing of mission critical voice over LTE networks.

An operational MCV capability includes a number of key functions[2], and successful implementation using LTE will require incorporation of a broad set of technologies, some of which are new or developing. However, PSCR's stakeholder engagement and

[2] See the National Public Safety Telecommunications Council report on Mission Critical Voice Communications Requirements for Public Safety

evaluation activities, coupled with the technology landscape assessments and industry roadmaps, clearly support the need for R&D in two particular areas: 1) direct mode operations, and 2) mission critical push-to-talk.

1. Direct Mode Operations

Direct mode operations (DMO) allow first responders to communicate independent of existing network infrastructure. DMO is currently used for several reasons, e.g., when operating outside of coverage areas or in covert mode, or in areas with limited or degraded network capacity. But, above all, it is a lifeline for first responders that allows them to communicate in emergencies and remote areas where other means are not available.

To address the critical public safety requirement for a direct mode broadband technology, as well as new modes of communication and discovery, the 3rd Generation Partnership Project (3GPP)[3] began to release LTE specifications in 2013 under the label Proximity Services (ProSe). Unlike conventional LTE in which transmissions are between base stations and devices via downlink or uplink, ProSe enables device-to-device (D2D) direct communication via a new channel called the 'sidelink'. ProSe further defines a method to extend network communications to out-of-coverage user equipment (UE) via the UE-to-network relay. ProSe also includes a 'direct discovery' feature that can be used to discover other users or devices in proximity. Though not yet formally released, specifications to enhance the sidelink to enable vehicle-to-vehicle (V2V) communications are also under development.

Despite this momentum, there are currently no ProSe-enabled products in the LTE marketplace that meet the requirements of public safety users. Thus, ProSe still needs to be studied carefully in conceptual and practical applications for DMO, both on-network and off-network. Furthermore, it is expected that ProSe, along with emerging 3GPP specifications to support Internet-of-things (IoT) communication, will enable a first responder to contact any and all resources, including people, devices, and machines, within their proximity via the broadband network to ensure robust communications and augment current-day operations.

The PSIAP seeks applications for R&D projects to stimulate commercial and technical organizations to create and support a market that will accelerate the development and adoption of DMO capabilities in public safety broadband devices, networks, applications, and operations. Examples (in no particular order) of possible R&D projects in this area include, but are not limited to:

a) Studying service continuity, i.e., how to enable seamless communications and network access as users and groups transition through in-coverage, partial coverage, and out-of-coverage scenarios using technologies like ProSe direct communications and UE-to-network relay. Questions that might be considered include:

[3] For more information on 3GPP see http://www.3gpp.org/about-3gpp/about-3gpp

(1) Are there any architecture and design considerations to enable service continuity between operational environments beyond the reference architecture model as identified in 3GPP TS 23.303[4].
(2) In providing service continuity, what factors must be considered when using scheduled resource allocation versus autonomous resource selection?
(3) If automating the transition between network and direct mode operation, what factors and key performance indicators (KPIs) should be considered by an algorithm that would trigger the changeover? What would be the impact on the user experience (e.g., handover delay, packet loss)?

b) Implementing a full LTE UE stack that includes ProSe on a programmable system-on-a-chip that could be integrated in public safety devices.
c) Developing accurate uplink/sidelink coexistence traffic models for predicting and verifying network performance, building on some of the work documented in 3GPP TR 36.877[5].
d) Developing test cases for ProSe that can be used by PSCR to test performance and conformance and be submitted for consideration by 3GPP for inclusion in conformance specifications like TS 36.521 and TS 36.523.
e) Developing methods to measure user quality of service and experience in an operational environment while operating in direct mode.
f) Conducting market research on how D2D technologies like ProSe might be adopted by consumers for applications like wearables, two-way radio, IoT, etc., and leveraged by commercial networks for carrier offloading, reduced backhaul, etc. Then further evaluating how this new mode of operation could be monetized and managed by commercial cellular operators, with the end-benefit for public safety being an economy of scale that could lower the cost of DMO-enabled public safety devices.
g) Studying how ProSe direct communication, and a related capability ProSe discovery, can be utilized to augment LBS technologies and public safety analytics.
h) Assessing the benefits, risks, and vulnerabilities of DMO technologies from a security perspective.
i) Developing enhancements to test equipment (e.g., base station emulators, load-testers) and software tools (e.g., Wireshark dissector, modeling and simulation, software defined radio frameworks) to facilitate test and measurement of DMO technologies in LTE networks.

2. Mission Critical Push-to-Talk

First responders use push-to-talk (PTT) technology as their standard communications for everyday operations. PTT allows users to push a button to (nearly instantaneously) initiate a transmission that can be broadcast to other users in a ‘talkgroup’, then release the button when done to hear transmissions from other users in the group. Beyond the PTT functionality, there are a range of other important capabilities and features that a public safety communications system must provide. To accommodate mutual aid

[4] Proximity-based Services (ProSe); Stage 2; v14.0.0; http://www.3gpp.org/DynaReport/23303.htm
[5] LTE Device to Device Proximity Services; User Equipment Radio Transmission and Reception; http://www.3gpp.org/DynaReport/36877.htm

scenarios these services must also have standard interfaces to be interoperable across public safety networks, and all of these capabilities, features, and interfaces must perform at a high level of reliability to support 'mission critical' first responder operations.

To address the critical public safety requirement of a mission critical broadband PTT capability, the 3GPP began to release LTE specifications for public safety PTT in 2016 under the label Mission Critical Push-to-Talk (MCPTT). In addition to providing the essential services and features, one of the primary goals of the MCPTT standard is to enable nationwide interoperability, a more competitive marketplace, and rapid technology migration at a scale not previously realized by current public safety networks and organizations. While there is a rich industry base supporting PTT communications in 'narrowband' land mobile radio (LMR) networks, the broadband PTT market is still relatively nascent. Emerging solutions will require significant testing and evaluation to ensure they meet the rigorous demands of a mission critical network.

The PSIAP seeks applications for R&D projects to accelerate the creation and adoption of MCPTT in public safety broadband devices, networks, applications, and operations. Examples (in no particular order) of possible R&D projects in this area include, but are not limited to:

a) Developing standards-based MCPTT application servers and clients that can be used as reference implementations across the public safety industry for prototypes to begin testing and evaluation.
b) Researching and developing standards-based interfaces between independent MCPTT application servers that will allow first responders in different networks, using different PTT applications and devices to communicate without having to download new applications or deploy additional network resources.
c) Developing or enhancing devices and equipment with appropriate hardware and software features to enable end-to-end MCPTT applications and services.
d) Participating in the MCPTT plug-tests organized by the European Telecommunications Standards Institute.
e) Leading an open source software project to develop an application programming interface (API) for the Android operating system to enable seamless integration of MCPTT and other features for public safety devices.
f) Developing APIs and middleware for MCPTT to enable rapid deployment of applications that rely on mission critical services.
g) Developing KPIs and supporting test methodologies for evaluating LTE MCPTT capabilities and technologies against similar benchmarks in LMR systems.
h) Developing a framework and data specification for integrating sensors, analytics, and decision thresholds into MCPTT applications.
i) Studying and demonstrating the potential benefits and risks to public safety operations if adaptive/dynamic floor control integrating real-time feedback from devices, sensors, and personnel is utilized.
j) Developing a test plan for expected battery life tailored to the operational requirements of first responder devices that includes consideration for ProSe,

evolved multimedia broadcast/multicast services (eMBMS), location based services, and personal area networks.

k) Developing enhancements to test equipment and software tools to facilitate test and measurement of MCPTT technologies in LTE networks.
l) Studying security aspects of MCPTT to include protecting the signaling, media, and identity of users.

B. Location Based Services

Emergency responders have a compelling need to understand the physical environment in which they are working: Where are public safety personnel and equipment? What hazards and resources are present in the area? What entry and exit routes are available? PSCR refers to the collection of technologies and systems that gather, store, disseminate, and act on location and located information as Location Based Services (LBS).

1. Positioning

The most fundamental component of LBS for public safety is positioning: The ability to determine where something or someone is, especially the ability to locate public safety personnel and assets that are working in highly dynamic, potentially dangerous environments. A successful positioning system will be one that can determine personnel positions in three dimensions with sufficient precision, accuracy, timeliness, and reliability across the widest possible range of environments. The definition of “sufficient” will vary between use cases and situations, but a minimum level of performance is a sub 3 meter error radius to be within 95% radius probability and sub 1 second refresh rate (that is, at any given time, the most recent estimated position corresponds to the true position at a time less than 1 second ago) indoors, including in the basement of, a large building. Note that this level of performance is what is required for first responder operations and should be distinguished from the positioning requirements in the Next Generation 9-1-1 initiative, which are for locating members of the public when responding to emergencies. The PSIAP seeks applications for:

a) Developing positioning systems that can determine responder locations to sufficient accuracy and timeliness in indoor environments. These systems may rely on any mix of sensors and technologies, but must not depend on the location where an incident occurs having been prepared in advance, for example by installing transmitters or receivers within the structure. Applications are welcome at any level of technological maturity.
b) Developing positioning systems that can determine the location of other assets (e.g., equipment brought by emergency personnel or pre-installed in the environment), and people (e.g., patients or trapped persons) with similar accuracy and under similar constraints.

2. Dissemination

A closely related component of LBS is position dissemination: the ability to get position information from the device(s) where it is calculated to the people who need to know it. It is frequently necessary to know where someone else is, for example to warn a person who is in danger, or to rescue a person who is incapacitated. Emergency responders

frequently work in environments in which communication is impaired; for example, it should not be assumed that infrastructure-based wireless communication is always available, or that there is a low-interference, low-attenuation radio path between all pairs of responders. A successful position dissemination system will be one that delivers sufficiently accurate and timely position information, reliably, across the widest possible range of communication environments. The PSIAP seeks applications for:

a) System-level research and development on position dissemination systems appropriate to public safety use. Software defined application architecture optimized based on network, device, power and server performance. A strong system-level proposal will address objectives of timeliness, reliability, accuracy, and security while considering communication, networking, and computation challenges.

3. Data Security, Integration, and Interoperation

The next layer of LBS is data security, integration, and interoperation: It is not enough to know locations of individual objects and people in some arbitrary coordinate system; it must be possible to integrate and derive meaningful information from a variety of data sources. The PSIAP seeks applications to assess, develop, and enhance the following capabilities:

a) Combining existing indoor and outdoor maps, drawings, imagery, and data in a way that is seamless to the user and presentable on a range of devices with a variety of form factors and display sizes, e.g., smartphones, tablets, and mobile data terminals.
b) Integrating data of variable provenance and confidence, for example publicly-sourced observations, responder-generated real-time updates, maps of varying age and quality, etc. This includes tracking the origin of information, and enabling users to make real-time selections of which sources to trust (and to what extent).
c) A framework for protecting the privacy, identity, and integrity of metadata related to location of first responders utilizing LBS systems, as well as authentication of, and access to, different LBS sources based on identity of users and operational scenarios.

4. Mapping and Visualization

PSCR is interested in data collection (mapping) and data output (visualization and other UI modalities). The PSIAP seeks applications for:

a) Assessing and developing tools and techniques for indoor mapping, including automatic visual (or other) SLAM (Simultaneous Location and Mapping). Of particular interest are approaches for first responder pre-planning (in which response plans are developed in advance for known high-risk events / locations) as well as “on-demand” mapping in unplanned events. Relevant issues include interoperability for large-scale indoor/outdoor building mapping, accuracy, error correction, user learning curve, and system cost.
b) Developing techniques for mapping and localizing personnel within outdoor covered areas in which traditional GPS and visual aerial imagery are insufficient. Examples include under water or snow, heavily forested areas, and caves. Of particular

interest are techniques based on (satellite or UAV) aerial measurement, including ground-penetrating RF and multi/hyperspectral imaging.

c) Addressing visualization of building and integration of vital information (e.g., sensors, HVAC and equipment, IoT devices, emergency equipment etc.). One example would be to create a Building Management Platform app that encourages building owners to make their own maps that can be utilized on a daily basis for building owners as well as for emergencies and requires zero technical expertise to set up or operate.

5. Affordable Localization Reference Environments

PSCR conducts internal research and development, with a heavy emphasis on testing and verification. We seek to test new localization technologies in realistic indoor scenarios with known "ground truth" location, and to accurately attribute location information to (other) measurements recorded while responders move around indoor environments. Thus, we are interested in ways that a controlled environment can be affordably instrumented to create a precise localization reference grid that can then be used to test a variety of LBS technologies and solutions. The reference environment should enable precision localization of persons or objects moving freely within the space, without requiring them to alter their behavior in order to be accurately tracked.

There are two application scenarios of interest, with somewhat different requirements: The first is in an "LBS testbed" which will be a benign indoor environment. The second is in collecting measurements during response training and simulations. In the second case, the more robust the system is to adverse environments, the more broadly useful it will be.

The PSIAP seeks applications for:

a) Developing cost-effective reference measurement systems that can be installed in controlled indoor environments (i.e. testbeds, public safety training facilities, etc.) and used to assess the accuracy of LBS solutions in determining the location and movement of personnel and their equipment progressing within the test environment. While such tools need not be robust enough for field use, there is added value in being suitable for use in challenging environments such as a fire simulator or controlled burn.

PSCR has published an LBS roadmap[6] and an LBS summit report[7] which may inform proposals addressing this technology area.

C. Public Safety Analytics

Over the next decade, as public safety's use of mobile broadband technologies increases, first responders will gain unprecedented access to 'big data' and data analytics that can be both collected from, and delivered to, mobile devices and sensors. While there is no doubt analytics will play an increasingly important role in the future public safety communications ecosystem, solutions are needed to address the volume,

[6] http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1883.pdf
[7] http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1914.pdf

variety, velocity, veracity, validity, and volatility of data. In order to further the creation and consumption of potentially transformational operational analytics capabilities for first responders, the PSIAP seeks applications for R&D projects to address three specific needs: 1) data sets, 2) analytics tools and frameworks, and 3) data analysis applications.

Proposals should demonstrate forward-looking, innovative R&D focused on solving novel challenges posed by the criticality and complexity of the data relevant to the public safety operational environment. The PSIAP is looking for R&D that will leverage new capabilities in the Nationwide Public Safety Broadband Network to circulate a rich diversity of data created by a variety of sensors, devices, and communications, and will harness the enormous computing power of potentially millions of edge-enabled devices to optimize and transform the flow of real-time actionable information to first responders and incident commanders.

Letters of commitment from public safety team members are required for proposals addressing the analytics technology area. For purposes of this NOFO, public safety includes U.S. federal, state, and local emergency medical services, fire services, and law enforcement.

1. Data Sets

Data sets collected from multiple sources and sensors that have been organized, integrated, and annotated, and that could be maintained for reuse by data scientists, analysts, and researchers are needed to develop meaningful public safety analytics techniques. Both static and dynamic data could be taken from real-world public safety, government, or open source information systems, or generated via simulations and training exercises. If the latter, consideration should be given not only to known or understood scenarios, but also to forward-looking, futuristic scenarios that are difficult to imagine but may enable more predictive and preventative analyses.

2. Analytics Tools and Frameworks

Tools are critically needed to make the development and tuning of analytic technologies more agile and less expensive so that it is easier for public safety to engage in the R&D process and share their analytic models and test methodologies across jurisdictions. To accomplish this, the public safety community requires a common R&D framework to support in situ development. Such a framework requires modular tools and a highly usable, interactive development environment to support data sharing, data integration, data curation, model development, user feedback and adaptation, and should incorporate both component and system level measures of uncertainty.

The framework needs to be extensible across domains and jurisdictions, and should make collaboration and sharing of use cases and best practices seamless throughout the entire workflow. This includes data transfer, storage, and management with an eye to the security, sharing, authenticity/provenance, and usability needs of public safety. The framework should encourage the use of common taxonomies and KPIs. In addition, the framework should include tools to optimize distributed processing that can leverage computational resources at the edge (e.g., servers attached to base stations, smart

phones) to reduce backhaul requirements and allow near real-time processing even when networks become disconnected or isolated (*see* also Section I.F.4: Service Replication and Access). This R&D framework would support innovation across academia, industry, and public safety, provide a common platform for rigorous performance measurement, and support future open interoperability standards.

3. Data Analytics

Analytics is inherently a massive technology area, which was reflected in the PSCR Public Safety Analytics Technology Roadmap. In order to narrow the scope, PSCR hosted a two-day Public Safety Analytics Summit with stakeholders to identify key problem statements deserving of more focused investment. PSCR wishes to build on these results by soliciting innovative exploratory, confirmatory, and qualitative data analytics for specific domains that are critically important to public safety. Proposals should consider how computing and communication resources can be effectively and dynamically optimized to enable robust, efficient, and real-time applications. In addition, proposals should consider how large volumes of complex data flowing through the public safety communications ecosystem can be effectively filtered to distill accurate, essential, and actionable information for first responders. Applicants should consider the legal obstacles, as well as governance and policy issues often encountered when attempting to access and share raw data in the public safety community, and propose innovative ways to develop meaningful applications despite these challenges.

D. Public Safety Communications Demand Model

To effectively evaluate current and future communication technologies for first responders, the research community needs a well-founded modelling framework specific to the user community’s needs. To be adequate, this framework should include more than simply the number of calls or volume of data. A demand model framework for public safety needs to capture the essence of how public safety communicates by documenting present and future modes of communication, usage needs in dynamic situations, urban and rural applications of similar technologies, etc. A demand model for public safety needs to enable researchers to answer questions such as "what kind of connection can a particular access network offer to a particular user at the moment when they need to communicate?" and "If this communication fails or is degraded, how operationally harmful is that?".

The PSIAP seeks applications for R&D projects to aid in the establishment of a cohesive public safety communications demand model framework, and to document and model public safety communication patterns and requirements, both in current practice and desired future capabilities. Proposals that either attempt to address the entire problem or specific parts will be considered. Example objectives for R&D projects include, but are not limited to:

a) Developing a library of incidents and scenarios, recorded in as much detail as possible. This can include both actual events and simulated or planned responses to hypothetical events.
b) Documenting modes of Public Safety communications, both present and desired future states.

c) Deriving probabilistic models that can generate realistic-enough communication demands to drive simulations of different scenarios.
d) Aggregating data on the (typical and worst-case) mix of events occurring within any given geographic area.
e) Developing and evaluating statistical models of aggregate demand.
f) Developing methods and tools for future modeling of public safety communication.

The PSIAP considers the following to be the key metrics of success for communication demand modeling R&D projects:

- The demand model framework should enable benchmarking against which a real or proposed communication system can be evaluated.
- The demand model framework should enable planning and provisioning of operational networks so that public safety users' needs are actually met.
- The demand model framework should serve as a common reference for modeling responses to specific Public Safety incident response scenarios.

The following questions and considerations are examples of the kind of information that may be addressed in a public safety communications demand model. It should not be viewed as a checklist, but rather indicative of the type of information that the PSIAP believes to be important.

a) Who is communicating with whom?
   - Individual and group communications.
   - What are the parties' roles / functions?
   - In groups, who is the information actually intended for?
b) Where are the parties physically?
c) What kind of communication is it, technically?
   - Voice, video, images, other data.
   - Full-duplex vs. half-duplex.
   - Interactive vs. one-way.
   - Real-time vs. non-real-time.
   - Quality of Service (QoS) needs (e.g., tolerance to jitter, dropped packets, latency, throughput reduction / variability).
   - Magnitude (e.g., minutes, megabytes, activity factor)?
   - Note that for modeling technical communication aspects, it is essential to distinguish between user needs (e.g., "video quality comparable to X") and implementation-specific properties (e.g., "2.5 Mbps streaming"). This is especially relevant to the immediately preceding two bullet points.
d) What kind of communication is it, operationally?
   - How critical is it / what are the consequences of failure?
   - How tolerant of delay?
   - How tolerant of (e.g., image/video/audio coding) quality reduction?
   - How does it relate to the events going on in the real world?

E. Research and Prototyping Platforms

Over the next decade, the public safety community will significantly increase their use of communications technologies to include: LTE mobile broadband, wireless backhaul for cellular systems, interworking, and positioning/LBS. The PSIAP seeks applications for R&D projects to create a baseline of research and prototyping platforms, i.e. systems, software, tools, and models, that minimize the additional effort and risk required to conduct new investigations focused on these public safety communication technologies.

1. To be effective as research and prototyping platforms, the following characteristics are desirable**:**

a) Ease of use as delivered.
b) Ease of programming new capabilities, including:
   (1) Clarity of code base.
   (2) Code modularity and reuse between components.
c) Clarity and completeness of documentation. Adequate documentation must include both:
   (1) “External” documentation, describing the interfaces by which the tool provided can be used without understanding its internal implementation, for instance the APIs by which a component might be configured, or the hooks by which a user might add a new component into the system.
   (2) “Internal” documentation, describing how the tool is implemented, in sufficient detail that subsequent developers can readily understand and change it.
d) Long-term sustainability: It is desirable for the platform – meaning both any existing platform extended for PSIAP and the enhancements made under it – to continue to be developed, maintained, and used beyond the end of this funding. Factors such as user and developer community, business models, governance structure, etc., may be relevant.
e) Development ecosystem: It is desirable for the work products generated under PSIAP awards to be usable within, and ideally share overlapping users, developers, conceptual structure, development model, programming languages and data formats etc., with a larger “ecosystem” of related research tools. Outputs produced by awardees should be openly available and transferrable to subsequent researchers using the tools developed as part of the PSIAP.
f) Availability for follow-on research: The work products generated by PSIAP recipients should be as widely usable for related research and development as possible. Suitability for both academic / non-commercial and industrial / commercial researchers is important.
g) Potential for commercialization: To the extent that the platform implements features of potential commercial value, it is desirable for there to be a path by which either the original implementer or some 3rd party can bring those features to market.

2. The PSIAP has identified the following four technologies as priorities for modeling, simulation, and prototyping; other technology areas may also be proposed. While broad 'coverage' of each technology area is desirable, few systems, whether for research or commercial purposes, fully implement every aspect or feature of a particular technology. The following list identifies specific aspects that are of particular interest to the PSIAP.

a) LTE Mobile Broadband - "LTE" here refers to the set of standards for mobile broadband (cellular) communication being developed by the 3rd Generation Partnership Project (3GPP), from Release 8 through work items under current consideration for future releases.
   (1) Quality-of-service (QoS), priority, and preemption (QPP).
   (2) Proximity Services (ProSe), especially off-network and out-of-coverage.
   (3) Implementations of Evolved Multimedia Broadcast/Multicast Service (eMBMS) including multimedia broadcast single frequency networks (MBSFN) and single-cell point-to-multipoint (SC-PTM).
   (4) Carrier aggregation.
   (5) IP Multimedia Subsystem (IMS) and voice-over-LTE (VoLTE).

b) Wireless Backhaul for Cellular Systems - This is of interest for simulation and modeling proposals, not for SDR prototyping tools.
   (1) Terrestrial point-to-point microwave.
   (2) Satellite data links.

c) Interworking
   (1) LMR-to-LTE gateways.

d) Positioning and LBS - While not strictly a communication technology, positioning and location-based services are of considerable interest and are often closely coupled to communication systems. Projects to jointly and accurately simulate both communication and positioning in realistic, especially indoor, environments, are welcome. These should be:
   (1) Consistent and interoperable modeling of device and user position and mobility within built environments.
   (2) Environment-specific models of positioning systems, especially with regard to accuracy, availability, and timeliness.

3. To expand or, in some cases, create research ecosystems in support of PSCR's mission, the PSIAP seeks projects to assess, develop, or enhance tools for modeling, simulation and prototyping of public safety communication technologies. Key priorities (in no particular order) for research and prototyping platforms include, but are not limited to:

Link/Physical-Level Simulators
Link-level simulators are used to study the communication performance of a physical radio link with respect to block error rate (BLER), throughput, spectrum efficiency, etc. Some desired characteristics of a link-level simulator are:

a) Realistic and sufficiently-complete implementation of LTE physical layer for device-to-device (D2D) and Vehicle-to-Anything (V2X) communications.
b) Physical layer simulation should be modular to be able to replace any component in the physical layer processing chain.
c) Channel models (propagation model, large scale and small scale fading) for public safety application scenarios to support D2D and V2X communications.
d) Provide flexible waveform generator functionality.
e) Support parallel computing capability.
f) Link layer simulation results should be easily adopted by packet-level network simulator.

Packet-Level Network Simulators
Packet-level simulators are discrete event simulators that model the end-to-end processing of data and control packets through all of the relevant devices and protocols in a (simulated) network. Some desired characteristics of a packet-level simulator are:

a) Realistic and sufficiently complete implementation of data and control protocols.
b) Realistic and sufficiently complete implementation of physical layer, especially public-safety-specific enhancements for LTE.
c) Ability to simulate networks at the scale of tens to hundreds of wireless devices.
d) Ability to simulate networks which combine the wireless technologies identified above with standard internet protocol (IP) networks.
e) Accuracy (and validation) of performance and error models.
f) Accuracy, detail, and consistency of channel models.
g) Inter-technology coexistence models – that is, to the extent that multiple wireless technologies are supported by a simulator, their interaction (if any) must be modeled reasonably.
h) Support dynamic networks, traffic models, and visualization capability for public safety scenarios.
i) Support performance metrics related to both quality of service (QoS) and qualify of experience (QoE), for communication types for which those are well-defined.

Software Defined / Programmable Radios
A programmable or software-defined radio (SDR) is a combination of hardware, middleware, and software that implements over-the-air radio frequency communication in a flexible, easily-modifiable way. SDR systems have dual value as prototyping tools in

their own right and as possible stepping stones toward operational, deployable implementations. Some desired characteristics of an SDR platform are:

a) Sufficiently complete implementation of RF and protocol stacks.
b) A sufficient set of interoperable components to complete realistic communication tasks and exercise major protocol features. For example, for an LTE system, this would mean UE, evolved node B (eNB), and evolved packet core (EPC) implementations.
c) Interoperability with existing devices and services.
d) Performance comparable to existing or likely operational implementations – that is, to the extent possible, experimental results obtained using the SDR platform should be valid predictors of operational system performance.
e) Ability to implement a network on the scale of two to ten devices, including greater than one base station / eNB.
f) Plausible path – technologically and commercially – toward operational implementation of features developed for the SDR.

F. Resilient Systems

Public Safety services and mission critical systems must be available and function properly in situations of poor network connectivity due to either routine faults or catastrophic events, whether man-made or natural disasters. Examples of resilient systems and services include: voice communication among responders; read access to existing data sets (e.g., maps, databases, imagery, reference material); write access to shared data (e.g., a responder or dispatcher enters information, or a sensor generates data, that is available to other public safety personnel); information intake from the general public; information output to the general public; and computation & data services (e.g., GIS, CAD, analytics).

The PSIAP seeks applications for R&D projects to evaluate or enhance the resilience of public safety mission critical systems in the face of connectivity challenges. This includes traditional research, evaluation prototypes, and enhancements to existing systems. The scenarios and research areas identified below are not exhaustive or authoritative: Identifying and evaluating critical services and connectivity threats, in both current and future use, is itself a significant area for research.

The following scenarios, offered for the purposes of illustration, are examples of situations where a ‘resilient’ system must continue to function.

- A group of responders goes into an area without fixed-base-station coverage. Their devices are able to communicate with each other (e.g., using LTE D2D functionality), but only with each other.
- A group of responders in an area of poor coverage can directly communicate with a vehicle-carried small base station which may have some attached computing devices. The base station may have backhaul to a fixed network (e.g., by LTE, mobile satellite, or otherwise), but backhaul may be intermittent, of very low throughput, or entirely absent.

- A large incident (for example, a major wildfire) occurs in an area without fixed network coverage. Responding agencies bring in multiple large base stations (e.g., LTE cells-on-wheels) and significant computing equipment. Infrastructure connections within this incident-area network (e.g., base station to base station, base station to command post, base station to laptops/servers) exist and are generally good, but may be limited or intermittent. Responders may or may not be within base station coverage at any particular time. Satellite backhaul will likely exist but the bandwidth-per-user will be negligible. Additional connections of opportunity (e.g., commercial cellular and internet) may or may not exist.
- An attacker (or inadvertent misconfiguration) jams key radio frequencies in an urban area. Wired infrastructure and alternate wireless infrastructure exists, but the preferred wireless technology (e.g., LMR, LTE band 14, LTE in general) is unavailable.
- A hurricane or earthquake causes major physical damage to a large area. Wireline power and network connections are unavailable for a significant period of time, and many or all fixed base stations and repeaters may be destroyed. Satellite backhaul may or may not be available. Local connectivity is established piecemeal as deployable resources are brought in, but these "islands" of connectivity may have poor or no connection to each other or national/remote networks.

The PSIAP considers the following research areas to be important in the area of resilient systems:

1. Decentralizing LTE/IMS Control and Data

This means that: (a) necessary services and functions are available within each "island" in the event of network partition / disconnection, and appropriate local replicas are used when necessary, with as little disruption as possible; (b) necessary databases are replicated, allowing for local modification as operationally necessary, with appropriate consistency; (c) both 3GPP and IP/PDN (packet data network) traffic, including session initiation protocol (SIP)/VoLTE/IMS control and data, are routed (and broken out) locally within any "island;" and (d) when the network is connected, but backhaul is limited (e.g., high latency, low throughput, or high cost/contention) user plane traffic and signaling traffic are kept local to the greatest extent possible.

2. Routing and Mobility Across Heterogeneous and Opportunistic Networks

An emergency network may be composed of multiple "domains," for example an operator-managed 3GPP component, pure IP over Ethernet and WiFi components, various IoT components, trunked land mobile radio, and various alternate point-to-point and point-to-multipoint radio links. LTE thoroughly supports UE mobility: For example, if a UE loses connection with its current eNB, it can attach to another one with minimal interruption. However, LTE offers less support for situations in which the other end of a connection must be changed; because the packet data network gateway (P-GW) is an "anchor" between the IP network and evolved packet system (EPS), if that anchor becomes unreachable (or inefficient to reach) from either side, it cannot be changed without substantial disruption. A given UE may be able to "break out" to the IP network in multiple places, but each breakout point has a separate IP address. IP-layer approaches (for example identifier-locator split architectures), and possibly integration

with LTE mobility and network status events, are desirable to maintain connectivity and efficient routing. Beyond routing, architectural questions of where and how IP-based networks and services (especially those not provided or managed by the NPSBN operator) are connected to the LTE network are applicable here.

3. Data Management, Access, and Consistency

It will frequently be the case that it is either impossible or impracticable for users to fetch data (and push changes) from/to a centralized authoritative repository (e.g., cloud and/or agency servers). Data should be replicated, both on demand and by pre-provisioning, to minimize load on overburdened radio access network (RAN) or backhaul links, and to ensure that critical data is available in disconnected situations. Client data requests should be satisfied from suitable replicas. Data access is not limited to read-only use of cached copies of an authoritative, remotely managed, data set: information will be generated by users and devices in the field, and such “edge-generated” data must also be available to other users in disconnected contexts. User-generated data can be both self-contained objects (e.g., “this is a photo taken by Officer X at time Y”) or edits to shared objects (e.g., “mark this bridge as washed out on everyone's map”). Additional desired capabilities include prioritizing data requests, use-case-informed quality selection / adaptation (e.g., “Would a lower-resolution, or lower-bitrate, or slightly-stale version be acceptable?”). Approaches from content-delivery networks (CDNs), information/content/data-oriented networks, and database and filesystem sharing, are likely to be relevant. A particularly important challenge in this context is security and control: where is data held; how is it secured, both at rest and in transit; and what metadata (about data objects, and who produces them, and who receives them) is shared, and how is that secured? If data adaptation and processing are done automatically in the network, how are confidentiality and integrity maintained?

4. Service Replication and Access

Most modern applications, especially cloud/mobile ones, rely on a mixture of centralized processing, shared (possibly centralized) data, and processing on the user device (e.g., phone or browser). Centralized/cloud processing generally brings two benefits: First, cloud servers have much greater resources (e.g., processing, working memory, storage, power, and bandwidth) than mobile devices, and second, the central process provides a point of application-specific coordination and control that would be challenging to provide at a data-store level. However, when the central server(s) are unreachable, cloud services fail. Geographic information systems (GIS) are a prime illustration: mobile clients can cache a small subset of data to do rendering and minimal analysis locally, but any significant processing, receiving data outside of the small cached set, or contributing data to others requires access to the cloud. It is therefore desirable to replicate services (as well as their associated data) to processing nodes which are close to, and reliably connected to, user devices. This invites questions of how services are replicated and hosted, what level of data consistency is maintained and how consistency is accomplished, how clients discover and select replicas, etc. Approaches from cloud and cloudlet computing, edge computing, and service-centric networking are likely to be relevant.

5. Future-Proofing

It is likely that the mechanisms developed under items 2,3, and 4 above will not be transparent for application developers; that is, software may need to be written differently to take advantage of them. However, application developers cannot and should not wait for those solutions to be mature before developing applications for use in the public safety broadband network. Consequently, there is a need for an evolutionary path by which systems developed in the near future can subsequently be upgraded to take advantage of advanced capabilities as they become available. Such a path might incorporate design and development guidelines, compatibility libraries, or other elements that have not yet been considered. An ideal approach would minimize both the initial burden on programmers (and performance penalty, if any) and the effort required to make subsequent upgrades.

6. Security, Identity, and Access Control

Many models of identity, permission, trust, and access management – including some being standardized for first responder mobile use – rely on access to remote servers holding policies, user data, and key material or shared secrets. Examples include a home subscriber server (HSS) in LTE, or an Identity Provider in federated identity systems. Without access to those servers, relying parties are generally forced to either deny all access requests (rendering systems nonfunctional) or blindly accept them (rendering them insecure). Neither outcome is desirable. We anticipate two sets of challenges: First, ensuring that services continue to function during periods of disconnection, reflecting the sets of principals and policies that were in place before disconnection. Second, securely allowing principals (users and devices) and policies to be added, removed, or changed during periods of disconnection. For example: If a new agency arrives on the scene of an off-network incident, can they be connected with the existing agencies? If a known person needs to be issued a new radio (or UE, or token, or whatever physical hardware holds identity and credential information for them) can that be done? If a new individual (one without existing digital identity information in the reachable servers) needs to be added to a team, can they? What equipment is needed to do this (e.g., a special/blessed management console, or can it be done on any UE/terminal)? Who has permission to do it? Is there an override mechanism if the normally-authorized parties are unavailable?

II. Federal Award Information

1. Funding Instrument

The funding instruments used in these programs will be grants or cooperative agreements, as appropriate. Where cooperative agreements are used, the nature of NIST's "substantial involvement" will generally include collaboration with the recipients in the scope of work.

2. Multi-Year Funding Policy

When an application for a multi-year award is approved, funding will usually be provided for only the first year of the project. If a project is selected for funding, NIST has no obligation to provide any additional funding in connection with that award. Continuation of an award to increase funding or extend the period of performance is at the sole

discretion of NIST. Continued funding will be contingent upon satisfactory performance, continued relevance to the mission and priorities of the PSIAP, and the availability of funds. Under this NOFO, NIST may elect to fully fund awards or to fund awards in accordance with the Multi-Year Funding policy.

3. Funding Availability

In FY 2017 through FY2019, NIST anticipates up to $30,000,000 may be available to fund awards in the range of $10,000 to $1,000,000 per year with project performance periods of up to two (2) years. Proposals submitted by institutions of higher education with the specific purpose of supporting research by students as part of their doctoral program may have performance periods of up to three (3) years. All awards will be made consistent with the multi-year funding policy (*see* Section II.2 of this NOFO).

III. Eligibility Information

1. Eligibility

All programs listed in this NOFO are open to all non-Federal entities. Eligible applicants include institutions of higher education, non-profit organizations, for-profit organizations, state and local governments, Indian tribes, hospitals, foreign public entities, and foreign governments. An eligible organization may work individually or include proposed subawardees, contractors or other collaborators. Please note that individuals and unincorporated sole proprietors are not considered "non-Federal entities" and are not eligible apply under this NOFO.

NIST will only consider one application per applicant; however, an applicant entity may be proposed as a subrecipient, contractor, or unfunded collaborator within applications submitted by other entities.

2. Cost Sharing or Matching

Matching funds are not required for this NOFO.

IV. Application and Submission Information

1. Address to Request Application Package

The application package is available at **www.grants.gov** under Funding Opportunity Number 2017-NIST-PSIAP-01.

2. Content and Format of Application Submission

a) Required Forms and Documents. The Application must contain the following:

(1) SF-424, Application for Federal Assistance. The SF-424 must be signed by an authorized representative of the applicant organization.

- SF-424, Item 12, should list the NOFO number 2017-NIST-PSIAP-01.
- SF-424, Item 18, should list the total Federal budget amount requested for the entire project.
- For SF-424, Item 21, the list of certifications and assurances is contained in the SF-424B.

(2) SF-424A, Budget Information - Non-Construction Programs. The budget should reflect anticipated expenses for the project, considering all potential cost increases, including cost of living adjustments.

The Grant Program Function or Activity on Line 1 under Column (a) should be entered as “Public Safety Communications Research Grant Program”. The Catalog of Federal Domestic Assistance Number on Line 1 under Column (b) should be entered as “11.609”.

These sections of the SF-424A should reflect funds for the first year of the award: Section A; Section B; Section C; and Section D. The budget estimate for the second year of the award should be entered in Section E, field 16, column (b).

Further details about this form can be can be found at:

http://www.grants.gov/web/grants/form-instructions/sf-424a-instructions.html .

(3) SF-424B, Assurances - Non-Construction Programs

(4) CD-511, Certification Regarding Lobbying. Enter “2017-NIST-PSIAP-01” in the Award Number field. Enter the title of the application used in field 15 of the SF-424, or an abbreviation of that title, in the Project Name field.

(5) SF-LLL, Disclosure of Lobbying Activities (if applicable)

(6) Technical Proposal. The Technical Proposal is a document of no more than twenty (20) pages total responsive to the program description (*see* Section I of this NOFO) and the evaluation criteria (*see* Section V.1 of this NOFO). The Technical Proposal should contain the following information:

(a) Executive Summary. This is an executive summary of the proposed project. The summary must explicitly state the objectives and approaches to meet those objectives, anticipated challenges, and benefits and impacts of the proposed project. This section must not include any proprietary or sensitive business information as NIST may make the executive summary available to the public after selection of awards. **The executive summary must not exceed one (1) single-sided page.** Any executive summary material provided beyond this page limit will be redacted and not considered by the reviewers.

(b) Project Description. This is a detailed description of the proposed project and should include:

i. A clear problem statement and well-defined objectives;
ii. A description of how the proposed R&D aligns with one or multiple key technology areas described in Section I. of this NOFO and how the R&D

will meet one or multiple objectives within the key technology areas relevant to the project;

iii. A technology assessment[8] that reflects the current state of the technology and the projected state of the technology as a direct result of successful project completion;
iv. Technology-specific KPIs and goals, as well as measurement techniques;
v. Functional architecture drawings and an explicit description of standards vs non-standards based interfaces, if applicable;
vi. Identification of anticipated outputs with a discussion of how the research and technology developed will be disseminated or made available; and
vii. Discussion of potential impacts to public safety.

Applicants with cross-cutting R&D projects should clearly identify the specific problems and objectives they are trying to solve and how these map to one or multiple PSCR technology areas in this section of their Technical Proposals.

This section will be evaluated in accordance with the following three evaluation criteria: *Strategic Alignment*, *Technical Acceleration*, and *Impact* (*see* Sections V.1.a, b, and c, respectively, of this NOFO). **The project description must not exceed ten (10) single-sided pages.** Any material provided beyond this page limit will be redacted and not considered by the reviewers.

(c) Project Execution. This section should provide clear and quantifiable milestones, timelines, and outputs that support the goals in the technical proposal. Technology transfer activities should not be included in this section, but rather in the Project Description, Section IV.2.a.(6).(b). Note the requirement in Section IV.2.a.(7).(d) for PSIAP recipients to attend the PSCR Public Safety Broadband Stakeholder Meetings each June during the term of the grant. Awardees will be required to send a minimum of one team member to the meetings to meet with stakeholders and present key plans and findings of their work to date. These meetings should be included in project timelines and budgets. Costs for this, and any other travel, must be included in the budget form SF-424A (*see* Section IV.2.a.(2) of this NOFO) and described in the budget narrative (*see* Section IV.2.a.(7) of this NOFO).

This section will be evaluated in accordance with the *Project Execution* evaluation criterion (*see* Section V.1.d of this NOFO). **The project execution must not exceed three (3) single-sided pages.** Any material provided beyond this page limit will be redacted and not considered by the reviewers.

[8] Applicants should use NASA's Technology Readiness Levels to define current and projected state, where applicable. The assessment must address the state of the art generally, not only the state of the applicants' own products and technology, and should also discuss the extent to which similar efforts are likely to be undertaken (by the applicants or others) without PSCR involvement.

(d) Qualifications and Resources Availability. This section should provide a detailed description of the qualifications of key personnel, both technical and managerial, who will be assigned to work on the proposed project. In addition, the applicant's experience with technology development and production should be described, as well as the applicant's access to the necessary staff, equipment, facilities, and overall support and resources to accomplish the proposed objectives. Examples of the applicant's demonstrated success on projects that are similar in scope and magnitude to the proposed project should be included in this section, if applicable. In addition, the applicant's plans to sustain and manage work related to or in support of the proposed project once the project is complete should be included.

A resume for the project leader is required. This individual is considered key personnel to the project. Resumes of additional key personnel may be supplied. Resumes are limited to 2 pages per individual and do not count toward the page limit for this section (see next paragraph).

This section will be evaluated in accordance with the *Qualifications and Resources Availability* evaluation criterion (*see* Section V.1.e of this NOFO). **The qualifications and resource availability must not exceed six (6) single-sided pages.** Any material, with the exception of key personnel resumes, provided beyond this page limit will be redacted and not considered by the reviewers.

(7) Budget Narrative. (This does not count toward the page limit). The Budget Narrative must provide a detailed breakdown of each of the object class categories as reflected on the SF-424A. The budget justification should address all of the budget categories (personnel, fringe benefits, equipment, travel, supplies, other direct costs and indirect costs) for which Federal funds are requested. The written justification should include the necessity and the basis for the cost. Proposed funding levels must be consistent with the project scope, and only allowable costs should be included in the budget. Information on cost allowability is available in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200 (http://go.usa.gov/SBYh), which apply to awards in this program. Information needed for each category is as follows:

(a) Personnel. At a minimum, the budget justification for all personnel should include the following: name, job title, commitment of effort on the proposed project in terms of average number of hours per week or percentage of time, salary rate, total direct charges on the proposed project, description of the role of the individual on the proposed project and the work to be performed.

(b) Fringe Benefits. Fringe benefits should be identified separately from salaries and wages and based on rates determined by organizational policy. The items included in the fringe benefit rate (e.g.,, health insurance, parking, etc.) should not be charged under another cost category.

(c) Equipment. Equipment is defined as an item of property that has an acquisition cost of $5,000 or more (unless the organization has established lower levels) and an expected service life of more than one year. Any items that do not meet the threshold for equipment can be included under the supplies line item. The budget justification should list each piece of equipment, the cost, and a description of how it will be used and why it is necessary to the successful completion of the proposed project. Please note that any general use equipment (computers, etc.) charged directly to the award should be allocated to the award according to expected usage on the project.

(d) Travel. For travel costs required by the recipient to complete the project, the budget justification for travel should include the following: destination; names and number of people traveling; dates and/or duration; mode of transportation, lodging and subsistence rates; and description of how the travel is directly related to the proposed project. For travel that is yet to be determined, please provide best estimates based on prior experience. If a destination is not known, an approximate amount may be used with the assumptions given for the location of the meeting.

PSIAP recipients will be required to send a minimum of one team member to the PSCR Public Safety Broadband Stakeholder Meetings each June during the term of the grant to meet with stakeholders and present key plans and findings of their work to date. The meetings are typically three to four days in length, but the exact dates and location of the meetings have not been determined at this time.

In addition, PSCR encourages applicants to consider other academic, industry, and public safety forums to present their work. Applicants that propose such activities should address the potential impact in the technical proposal.

Applicants should factor in the cost for attending these events in their budget narrative and SF424A form.

(e) Supplies. Provide a list of each supply, and the breakdown of the total costs by quantity or unit of cost. Include the necessity of the cost for the completion of the proposed project.

(f) Contracts/Subawards. Each contract or subaward should be treated as a separate item. Describe the services to be provided and the necessity of the subaward or contract to the successful performance of the proposed project. Contracts are for obtaining goods and services. Subawardees perform part of the project scope of work. For each subaward, applicants must provide budget detail justifying the cost of the work performed on the project.

(g) Other Direct Costs. For costs that do not easily fit into the other cost categories, e.g., publishing fees or software distribution expenses, please list the cost, and the breakdown of the total costs by quantity or unit of cost. Include the necessity of the cost for the completion of the proposed project. Only allowable costs can be charged to the award.

This section will be evaluated in accordance with the Project Execution evaluation criteria (*see* Section V.1.d of this NOFO). It will also be reviewed to determine if all costs are reasonable, allocable, and allowable under 2 C.F.R. Part 200 Subpart E, Cost Principles.

(8) Indirect Cost Rate Agreement. If indirect costs are included in the proposed budget, provide a copy of the approved negotiated agreement if this rate was negotiated with a cognizant Federal audit agency. If the rate was not established by a cognizant Federal audit agency, provide a statement to this effect. If the successful applicant includes indirect costs in the budget and has not established an indirect cost rate with a cognizant Federal audit agency, the applicant will be required to obtain such a rate in accordance with the Department of Commerce Financial Assistance Standard Terms and Conditions (http://go.usa.gov/hKbj).

Alternatively, in accordance with 2 C.F.R. § 200.414(f), applicants that have never received a negotiated indirect cost rate may elect to charge indirect costs to an award pursuant to a de minimis rate of 10 percent of modified total direct costs (MTDC), in which case a negotiated indirect cost rate agreement is not required. Applicants proposing a 10 percent de minimis rate pursuant to 2 C.F.R. § 200.414(f) should note this election as part of the budget and budget narrative portion of the application.

(9) Letters of Commitment. Letters of commitment are required for the Public Safety Analytics technology area and are optional for all other technology areas. Letters of commitment must be submitted by all funded and unfunded entities that will have an active role in executing the activities outlined in the technical proposal. Letters of commitment should address the level of participation, qualifications of the personnel who will be actively involved, and the potential impact on the field. Letters of commitment must be signed by an individual with sufficient authority to legally bind the organization to its commitment.

Letters of commitment will be evaluated in accordance with the *Impact* and *Qualifications and Resources Availability* evaluation criteria (*see* Section V.1.c). and e). of this NOFO). Letters of commitment do not count against the twenty (20) page limit of the technical proposal.

Any proposal addressing the Public Safety Analytics technology area must submit the letters of commitment as part of the application package. Any application that is missing required letters of commitment will be considered non-responsive, and the proposal will be eliminated from further consideration (*see* Section V.3.a. of this NOFO).

(a) Public Safety. Letters of commitment from public safety team members are required for proposals addressing the analytics technology area. This is to ensure that PSOs have an active role in defining and developing the highly relevant and impactful data sets, tools, and techniques expected from work funded by the PSIAP. Letters of commitment from public safety partners must address the potential impact for themselves and for public safety as a whole. For purposes of this NOFO, public safety includes U.S. federal, state, and local emergency medical services, fire services, and law enforcement. Please note that Federal entities are not eligible to receive funding under this NOFO though they may participate as unfunded collaborators.

(b) In order to facilitate impactful partnerships between industry and public safety, the PSIAP will maintain a list of PSOs that have expressed interest in participating in the PSIAP. Interested PSOs should send an e-mail to pscr@nist.gov expressing their interest along with their specific areas of expertise or concern, and points of contact. Potential applicants may request this information by sending an e-mail to pscr@nist.gov. Note that partnerships are not limited to only those PSOs and applicants who have submitted or requested information, i.e. any applicant can partner with any PSO, subject to the eligibility requirements in this NOFO. Applicants are encouraged to develop partnerships with PSOs on their own. Potential applicants are responsible for contacting the organizations and arranging partnerships. NIST will not assist potential applicants with finding partners.

(c) Other. Letters of commitment from non-PSOs are not required. However, if submitted they will be evaluated as indicated above. These letters of commitment can be from entities that are funded or unfunded partners that will have an active role in the performance of the technical proposal.

(10) Letters of support. Letters of support are not required but may be provided by any entity that has a shared interest in the proposal's success from a technological standpoint. Letters of support may not be provided by an entity proposed to be actively involved in the performance of the technical proposal.

Letters of support will be evaluated in accordance with the *Impact* and *Qualifications and Resources Availability* evaluation criteria (*see* Section V.1.c), and e). of this NOFO). Letters of support do not count against the twenty (20) page limit of the technical proposal.

(11) Data Management Plan. In accordance with the Office of Science and Technology Memorandum[9] for the Heads of Executive Departments and Agencies of February 22, 2013, *Increasing Access to the Results of Federally Funded Scientific Research*, and as implemented through NIST Policy 5700.00[10],

[9] https://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf
[10] http://www.nist.gov/data/upload/Final-P-5700.pdf

Managing Public Access to Results of Federally Funded Research, and NIST Order 5701.00[11], *Managing Public Access to Results of Federally Funded Research*, applicants should include a Data Management Plan (DMP).

The DMP is a supplementary document of not more than two pages that must include, at a minimum, a summary of proposed activities that are expected to generate data, a summary of the types of data expected to be generated by the identified activities, a plan for storage and maintenance of the data expected to be generated by the identified activities, and a plan describing whether and how data generated by the identified activities will be reviewed and made available to the public. As long as the DMP meets these NIST requirements, it may take the form specified by the applicant's institution or some other entity (e.g., the National Science Foundation[12] or the National Institutes of Health[13]).

All applications for activities that will generate scientific data using NIST funding are required to adhere to a DMP or explain why data sharing and preservation are not within the scope of the project.

For the purposes of the DMP, NIST adopted the definition of "research data" at 2 C.F.R. § 200.315(e)(3) (available at http://go.usa.gov/3sZvQ).

Reasonable costs for data preservation and access may be included in the application.

The sufficiency of the DMP will be considered as part of the administrative review (*see* Section V.3.a). of this NOFO); however, the DMP will not be evaluated against any evaluation criteria.

b) Attachment of Required Documents

Items IV.2.a.(1) through IV.2.a.(5) above are part of the standard application package in Grants.gov and can be completed through the download application process.

Items IV.2.a.(6) through IV.2.a.(11) must be completed and attached by clicking on "Add Attachments" found in item 15 of the SF-424, Application for Federal Assistance. This will create a zip file that allows for transmittal of the documents electronically via Grants.gov.

Applicants should carefully follow specific Grants.gov instructions at www.grants.gov to ensure the attachments will be accepted by the Grants.gov system. ***A receipt from Grants.gov indicates only that an application was transferred to a system. It does not provide details concerning whether all attachments (or how many attachments) transferred successfully.*** Applicants using Grants.gov will receive a

[11] http://www.nist.gov/data/upload/Final-O-5701_0.pdf

[12] http://www.nsf.gov/bfa/dias/policy/dmp.jsp
[13] http://grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm

series of e-mail messages over a period of up to two business days before learning whether a Federal agency's electronic system has received its application.

Applicants are strongly advised to use the Grants.gov Download Submitted Applications option to check that their application's required attachments were contained in their submission.

After submitting the application, follow the directions found in the grants.gov Online Users Guide (http://go.usa.gov/cjaEh). Click first on Applicants; then click on Applicant Actions; go then to the "Check My Application Status" option, and choose Download Submitted Applications.

If any, or all, of the required attachments are absent from the submission, follow the attachment directions found above, resubmit the application, and check again for the presence of the required attachments.

Applicants can track their submission in the Grants.gov system by following the procedures at the Grants.gov site (http://go.usa.gov/cjamz). It can take up to two business days for an application to fully move through the Grants.gov system to NIST.

NIST uses the Tracking Numbers assigned by Grants.gov, and does not issue Agency Tracking Numbers.

c) Application Format

(1) Paper, E-mail and Facsimile (fax) Submissions. Will not be accepted.

(2) Figures, Graphs, Images, and Pictures. Should be of a size that is easily readable or viewable and may be landscape orientation.

(3) Font. Easy to read font (12-point minimum). Smaller type may be used in figures and tables but must be clearly legible**.**

(4) Page Limit. Twenty (20) pages for the Technical Proposal, noting the following limits for each section of the Technical Proposal (*see* Section IV.2.a.(6) of this NOFO): Executive Summary one (1) page; Project Description ten (10) pages; Project Execution three (3) pages; Qualifications and Resources Availability six (6) pages excluding resumes.

(5) Page Limit Excludes: SF-424, Application for Federal Assistance; SF-424A, Budget Information – Non-Construction Programs; SF-424B, Assurances – Non-Construction Programs; CD-511, Certification Regarding Lobbying; SF-LLL, Disclosure of Lobbying Activities; Resumes of key personnel (although resumes are limited to two (2) pages each); Budget Narrative; Indirect Cost Rate Agreement, Letters of Commitment; Letters of Support; and the Data Management Plan.

(6) Page size. 21.6 centimeters by 27.9 centimeters (8 ½ inches by 11 inches).

(7) Application language. English.

d) Application Replacement Pages. Applicants may not submit replacement pages and/or missing documents once an application has been submitted. Revisions can only be made by submitting a complete new application that is received by NIST before the submission deadline.

e) Pre-Applications. Pre-applications are not required under this NOFO.

f) Statement of Intent. To assist NIST in gauging interest and planning for the evaluation process all potential applicants are strongly encouraged to send an e-mail to pscr@nist.gov indicating intent to apply, along with tentative topic areas. The statement of intent shall not be used as part of the evaluation process and shall not be used to eliminate any applicants from consideration under this NOFO. An applicant may still apply and receive full consideration under this NOFO if a statement of intent is not submitted

g) Certifications Regarding Federal Felony and Federal Criminal Tax Convictions, Unpaid Federal Tax Assessments and Delinquent Federal Tax Returns. In accordance with Federal appropriations law, an authorized representative of the selected applicant(s) may be required to provide certain pre-award certifications regarding federal felony and federal criminal tax convictions, unpaid federal tax assessments, and delinquent federal tax returns.

3. Unique Entity Identifier and System for Award Management (SAM)

Pursuant to 2 C.F.R. part 25, applicants and recipients (as the case may be) are required to: (i) be registered in SAM before submitting its application; (ii) provide a valid unique entity identifier in its application; and (iii) continue to maintain an active SAM registration with current information at all times during which it has an active Federal award or an application or plan under consideration by a Federal awarding agency, unless otherwise excepted from these requirements pursuant to 2 C.F.R. § 25.110. NIST will not make a Federal award to an applicant until the applicant has complied with all applicable unique entity identifier and SAM requirements and, if an applicant has not fully complied with the requirements by the time that NIST is ready to make a Federal award pursuant to this NOFO, NIST may determine that the applicant is not qualified to receive a Federal award and use that determination as a basis for making a Federal award to another applicant.

4. Submission Dates and Times

Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, Tuesday, February 28, 2017. Applications received after this deadline will not be reviewed or considered. **Applicants should be aware, and factor in their application submission planning, that the Grants.gov system is expected to be closed for routine maintenance from 12:01 Eastern Time, Saturday, December 17, 2016 until Monday, December 19, 2016 at 6:00 a.m. Eastern Time, and also from 12:01**

Eastern Time, Saturday, January 21, 2017 until Monday, January 23, 2017 at 6:00 a.m. Eastern Time, and again from 12:01 Eastern Time, Saturday, February 18, 2017 until Tuesday, February 21, 2017 at 6:00 a.m. Eastern Time . Applications cannot be submitted when Grants.gov is closed. NIST expects to complete its review, selection of successful applicants, and award processing by May 2017. NIST expects the earliest start date for awards under this NOFO to be June 1, 2017.

When developing the submission timeline, please keep in mind that: (1) all applicants are required to have a current registration in the electronic System for Award Management (SAM.gov); (2) the free annual registration process in the SAM.gov (*see* Sections IV.3. and IV.7.a.(1).(b). of this NOFO) often takes between three and five business days and may take as long as two weeks; (3) applicants are required to have a current registration in Grants.gov; and (4) applicants using Grants.gov will receive email notifications over a period of up to two business days as the application moves through intermediate systems before the applicant learns via a validation or rejection notification whether NIST has received the application. (See http://www.grants.gov for full information on application and notification through Grants.gov.). Please note that a federal assistance award cannot be issued if the designated recipient's registration in the System for Award Management (SAM.gov) is not current at the time of the award.

5. Intergovernmental Review
Applications under this Program are not subject to Executive Order 12372.

6. Funding Restrictions
Applications for product development and/or commercialization are not considered responsive to this NOFO. Profit or fee is not an allowable cost.

7. Other Submission Requirements

a) Applications must be submitted electronically.

(1) Applications must be submitted via Grants.gov at www.grants.gov.

(a) Applicants should carefully follow specific Grants.gov instructions to ensure that all attachments will be accepted by the Grants.gov system. A receipt from Grants.gov indicating an application is received does not provide information about whether attachments have been received. For further information or questions regarding applying electronically for the 2017-NIST-PSIAP-01 announcement, contact Christopher Hunton by phone at 301-975-5718 or by e-mail at grants@nist.gov.

(b) Applicants are strongly encouraged to start early and not wait until the approaching due date before logging on and reviewing the instructions for submitting an application through Grants.gov. The Grants.gov registration process must be completed before a new registrant can apply electronically. If all goes well, the registration process takes three to five business days. If problems are encountered, the registration process can take up to two weeks

or more. Applicants must have a valid unique entity identifier number and must maintain a current registration in the Federal government's primary registrant database, the System for Award Management (https://www.sam.gov/), as explained on the Grants.gov Web site. Also *see* Section IV.3. of this NOFO. After registering, it may take several days or longer from the initial log-on before a new Grants.gov system user can submit an application. Only individuals authorized as organization representatives will be able to submit the application, and the system may need time to process a submitted application. Applicants should save and print the proof of submission they receive from Grants.gov. If problems occur while using Grants.gov, the applicant is advised to (a) print any error message received and (b) call Grants.gov directly for immediate assistance. If calling from within the United States or from a U.S. territory, please call 800-518-4726. If calling from a place other than the United States or a U.S. territory, please call 606-545-5035. Assistance from the Grants.gov Help Desk will be available around the clock every day, with the exception of Federal holidays. Help Desk service will resume at 7:00 a.m. Eastern Time the day after Federal holidays. For assistance using Grants.gov, the applicant may also contact support@grants.gov.

(c) To find instructions on submitting an application on Grants.gov, Applicants should refer to the "Applicants" tab in the banner just below the top of the www.grants.gov home page. Clicking on the "Applicants" tab produces two exceptionally useful sources of information, Applicant Actions and Applicant Resources, which applicants are advised to review.

Applicants will receive a series of e-mail messages over a period of up to two business days before learning whether a Federal agency's electronic system has received its application. Closely following the detailed information in these subcategories will increase the likelihood of acceptance of the application by the Federal agency's electronic system.

Applicants should pay close attention to the guidance under "Applicant FAQs," as it contains information important to successful submission on Grants.gov, including essential details on the naming conventions for attachments to Grants.gov applications.

All applicants should be aware that adequate time must be factored into applicants' schedules for delivery of their application. Applicants are advised that volume on Grants.gov may be extremely heavy leading up to the deadline date.

The application must be both received and validated by Grants.gov. The application is "received" when Grants.gov provides the applicant a confirmation of receipt and an application tracking number. If an applicant does not see this confirmation and tracking number, the application has not been received. After the application has been received, it must still be validated. During this process, it may be "validated" or

"rejected with errors." To know whether the application was rejected with errors and the reasons why, the applicant must log in to Grants.gov, select "Applicants" from the top navigation, and select "Track my application" from the drop-down list. If the status is "rejected with errors," the applicant may still seek to correct the errors and resubmit the application before the deadline. If the applicant does not correct the errors, the application will not be forwarded to NIST by Grants.gov.

Refer to important information in Section IV.4. Submission Dates and Times, to help ensure the application is received on time.

b) Amendments. Any amendments to this NOFO will be announced through Grants.gov. Applicants may sign up on Grants.gov to receive amendments by e-mail or may request copies by e-mail from mailto:pscr@nist.gov.

V. Application Review Information

1. Evaluation Criteria

The evaluation criteria that will be used in evaluating applications and assigned weights are as follows:

a) Strategic alignment (0-20 points): Reviewers will evaluate the extent to which the proposed R&D:
(1) demonstrates a clear understanding of the challenges.
(2) aligns with the key technology areas.
(3) meets the objectives listed in the Program Description (*see* Section I of this NOFO).

b) Technical acceleration (0-30 points): Reviewers will evaluate:
(1) the likelihood that the project will evolve a technology or market from its current level[14] to a more advanced level, and the likely rate at which this acceleration will be achieved.
(2) the extent to which the technical approach is comprehensive, innovative, feasible, and likely to achieve the stated objectives.
(3) the appropriateness of the proposed technology-specific key performance indicators and goals.

c) Impact (0-30 points): Reviewers will evaluate:
(1) the potential impact that successful completion of the project would have on public safety end users and operations.,
(2) the likelihood that the results will be generally applicable for the public safety community, academia, and the industrial base.
(3) the likelihood that the research or technology being developed will affordably and quickly be made available to the public safety community.

[14] Applicants should use NASA's Technology Readiness Levels to define current and projected state, where applicable. The assessment must address the state of the art generally, not only the state of the applicants' own products and technology. This should include the extent to which similar efforts are likely to be undertaken (by the applicants or others) without PSCR involvement.

(4) the lasting value that the outputs and contributions would have for the industrial and academic base to continue and extend work in this area through direct access, interoperability, or other means.

d) Project Execution (0-10 points): Reviewers will evaluate the feasibility and appropriateness of the milestones, timelines, and budgeted costs with respect to executing the proposed project and meeting the stated objectives.

e) Qualifications and Resources Availability (0-10 points): Reviewers will evaluate:
(1) the qualifications of the key staff, leadership, and technical experts.
(2) the sufficiency, availability, and appropriateness of proposed facilities and resources.
(3) letters of commitment for the appropriateness of the partnership to PSIAP, their expertise, and their ability to contribute to the project.

2. Selection Factors

The Selecting Official, the Chief of the PSCR Division, shall generally select and recommend applications for award based upon the adjectival rankings (*see* Section V.3.b.(2 of this NOFO) of the applications. The Selecting Official may select and recommend an application for award out of rank order based on one or more of the following selection factors:

a) The availability of funding.
b) Whether the project duplicates other projects funded or considered for funding by NIST or other federal agencies.
c) Alignment with NOFO objectives and PSCR priorities.
d) Diversity within the PSCR R&D portfolio.
e) Regional diversity.

3. Review and Selection Process

Proposals, reports, documents and other information related to applications submitted to NIST and/or relating to financial assistance awards issued by NIST will be reviewed and considered by Federal employees, or non-Federal personnel who have entered into nondisclosure agreements covering such information, when applicable.

a) Initial Administrative Review of Applications. An initial review of timely received applications will be conducted to determine eligibility, completeness, and responsiveness to this NOFO and the scope of the stated program objectives. Applications determined to be ineligible, incomplete, and/or nonresponsive may be eliminated from further review. However, NIST, in its sole discretion, may continue the review process for an application that is missing non-substantive information, the absence of which may easily be rectified during the review process.

b) Full Review of Eligible, Complete, and Responsive Applications. Applications that are determined to be eligible, complete, and responsive will proceed for full reviews in accordance with the review and selection process below:

(1) Merit Review. At least three (3) objective reviewers, who may be Federal employees or non-Federal personnel, with appropriate professional and technical expertise relating to the topics covered in this NOFO, will evaluate and score each eligible, complete, and responsive application based on the evaluation criteria (*see* Section V.1 of this NOFO). While every application will have at least three reviews, applications may have more than three (3) reviewers if specialized expertise is needed to evaluate an application. During the review process, the reviewers may discuss the applications with each other, but scores and narrative comments will be determined on an individual basis. Reviewers may consult as a panel with Federal or non-Federal subject-matter experts to seek clarification or explanation of specific issues identified during the initial review process. The applications will then be ranked by averaging the scores of all reviewers for each application.

(2) Program Review. Following the merit review described above in Section V.3.b.i of this NOFO, a Programmatic Evaluation Panel, consisting of at least three (3) persons comprised of any mix of NIST staff and other federal employees with appropriate professional and technical expertise, will conduct a review of the merit reviewers' ranked applications. For the purpose of clarifying information in an application, the Evaluation Panel may ask questions of applicants in writing and/or may require teleconferences with all applicants. The Evaluation Panel will prepare and provide a final adjectival ranking of the applications to the Selecting Official (*see* Section V.2 of this NOFO) for further consideration, taking into consideration the following information:

(a) All application materials;
(b) Results of the reviewers' evaluations; and
(c) Any clarifying information obtained through written questions or teleconferences with the applicants.

The adjectival ratings are:

- Fundable, Outstanding;
- Fundable, Very Good;
- Fundable; or
- Unfundable.

If more than one application falls into a given adjectival ranking, then the applications will also be numerically ranked within each adjectival ranking, based on the average of their numerical scores from the Merit review (*see* Section V.3.b.(1) of this NOFO).

c) Ranking and Selection. The Selecting Official, Chief of the PSCR Division, will make final award recommendations to the NIST Grants Officer. Recommendations for awards will be made in rank order unless the Selecting Official determines that an application is justified to be selected out of rank order based upon one or more of the selection factors listed in Section V.2. of this NOFO.

NIST reserves the right to negotiate the budget costs with any applicant selected to receive an award, which may include requesting that the applicant removes certain costs. Additionally, NIST may request that successful applicants modify objectives or work plans and provide supplemental information required by the agency prior to award. NIST also reserves the right to reject an application where information is uncovered that raises a reasonable doubt as to the responsibility of the applicant. NIST may select some, all, or none of the applications, or part(s) of any particular application. NIST may request that applicants ranked fundable or higher work together in a combined project if this approach might effectively advance the program mission. The final approval of selected applications and issuance of awards will be by the NIST Grants Officer. The award decisions of the NIST Grants Officer are final.

d) Federal Awarding Agency Review of Risk Posed by Applicants. After applications are proposed for funding by the Selecting Official, the NIST Grants Management Division (GMD) performs pre-award risk assessments in accordance with 2 C.F.R. § 200.205, which may include a review of the financial stability of an applicant, the quality of the applicant's management systems, the history of performance, and/or the applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-Federal entities.

In addition, prior to making an award where the total Federal share is expected to exceed the simplified acquisition threshold (currently $150,000), NIST GMD will review and consider the publicly available information about that applicant in the Federal Awardee Performance and Integrity Information System (FAPIIS). An applicant may, at its option, review and comment on information about itself previously entered into FAPIIS by a Federal awarding agency. As part of its review of risk posed by applicants, NIST GMD will consider any comments made by the applicant in FAPIIS in making its determination about the applicant's integrity, business ethics, and record of performance under Federal awards. Upon completion of the pre-award risk assessment, the Grants Officer will make a responsibility determination concerning whether the applicant is qualified to receive the subject award and, if so, whether appropriate special conditions that correspond to the degree of risk posed by the applicant should be applied to an award.

4. Anticipated Announcement and Award Date

Review of Applications, selection of successful applicants, and award processing is expected to be completed by May 2017. The earliest start date for awards under this NOFO is expected to be June 1, 2017.

5. Additional Information

a) Safety. Safety is a top priority at NIST. Employees and affiliates of award recipients who conduct project work at NIST will be expected to be safety-conscious, to attend NIST safety training, and to comply with all NIST safety policies and procedures, and with all applicable terms of their guest research agreement.

b) Notification to Unsuccessful Applicants. Unsuccessful applicants will be notified by email.

c) Retention of Unsuccessful Applications. All electronic applications, whether successful or unsuccessful, are stored indefinitely in the NIST Grants Management and Information System.

VI. Federal Award Administration Information

1. Federal Award Notices

Successful applicants will receive an award package from the NIST Grants Officer. The award cover page, i.e., CD-450, Financial Assistance Award is available at https://connection.commerce.gov/sites/connection.commerce.gov/files/media/files/2016/cd-450.pdf

2. Administrative and National Policy Requirements

a) Uniform Administrative Requirements, Cost Principles and Audit Requirements. Through 2 C.F.R. § 1327.101, the Department of Commerce adopted Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200, which apply to awards in this program. Refer to http://go.usa.gov/SBYh and http://go.usa.gov/SBg4.

b) Department of Commerce Financial Assistance Standard Terms and Conditions. The Department of Commerce will apply the Financial Assistance Standard Terms and Conditions dated December 26, 2014, accessible at http://go.usa.gov/hKbj, to this award. Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if this link is no longer working or more information is needed.

c) Pre-Award Notification Requirements. The Department of Commerce will apply the Pre-Award Notification Requirements for Grants and Cooperative Agreements dated December 30, 2014 (79 FR 78390), accessible at http://go.usa.gov/hKkR. Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if this link is no longer working or more information is needed.

d) Funding Availability and Limitation of Liability. Funding for the program listed in this notice is contingent upon the availability of Fiscal Year 2017 appropriations. NIST issues this notice subject to the appropriations made available under the current continuing resolution funding the Department of Commerce, the Continuing Appropriations and Military Construction Veterans Affairs, and Related Agencies Appropriation Act, 2017 and Zika Response and Preparedness Act, Public Law 114-223 (September 29, 2016). NIST anticipates making awards for the program listed in this notice provided that funding for the program is continued beyond December 9, 2016, the expiration of the current continuing resolution.

In no event will NIST or the Department of Commerce be responsible for proposal preparation costs if these programs fail to receive funding or are cancelled because of agency priorities. Publication of this announcement does not oblige NIST or the Department of Commerce to award any specific project or to obligate any available funds.

e) Collaborations with NIST Employees. If an applicant proposes collaboration with NIST, the statement of work should include a statement of this intention, a description of the collaboration, and prominently identify the NIST employee(s) involved, if known. Any collaboration by a NIST employee must be approved by appropriate NIST management and is at the sole discretion of NIST. Prior to beginning the merit review process, NIST will verify the approval of the proposed collaboration. Any unapproved collaboration will be stricken from the application prior to the merit review. Any collaboration with an identified NIST employee that is approved by appropriate NIST management will not make an application more or less favorable in the competitive process.

f) Use of NIST Intellectual Property. If the applicant anticipates using any NIST-owned intellectual property to carry out the work proposed, the applicant should identify such intellectual property. This information will be used to ensure that no NIST employee involved in the development of the intellectual property will participate in the review process for that competition. In addition, if the applicant intends to use NIST-owned intellectual property, the applicant must comply with all statutes and regulations governing the licensing of Federal government patents and inventions, described in 35 U.S.C. §§ 200-212, 37 C.F.R. Part 401, 2 C.F.R. §200.315, and in Section D.03 of the DoC Financial Assistance Terms and Conditions dated December 26, 2014, found at http://go.usa.gov/hKbj.

Any use of NIST-owned intellectual property by a recipient of an award under this announcement is at the sole discretion of NIST and will be negotiated on a case-by-case basis if a project is deemed meritorious. The applicant should indicate within the statement of work whether it already has a license to use such intellectual property or whether it intends to seek one.

g) Research Activities Involving Human Subjects, Human Tissue, Data or Recordings Involving Human Subjects Including Software Testing. Any application that includes research activities involving human subjects, human tissue/cells, or data or recordings from or about human subjects, must satisfy the requirements of the Common Rule for the Protection of Human Subjects ("Common Rule"), codified for the Department of Commerce at 15 C.F.R. Part 27. Research activities involving human subjects who fall within one or more of the classes of vulnerable subjects found in 45 C.F.R. Part 46, Subparts B, C and D must satisfy the requirements of the applicable subpart(s). In addition, any such application that includes research activities on these subjects must be in compliance with all applicable statutory requirements imposed upon the Department of Health and Human Services (DHHS) and other Federal agencies, all regulations, policies and guidance adopted by DHHS, the Food and Drug Administration (FDA), and other

Federal agencies on these topics, and all Executive Orders and Presidential statements of policy on applicable topics. (Regulatory Resources: http://www.hhs.gov/ohrp/humansubjects/index.html which includes links to FDA regulations, but may not include all applicable regulations and policies).

NIST uses the following Common Rule definitions for research and human subjects research:

Research: A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes. For example, some demonstration and service programs may include research activities.

Human Subject: A living individual about whom an investigator (whether professional or student) conducting research obtains data through intervention or interaction with the individual or identifiable private information.

(1) *Intervention* includes both physical procedures by which data are gathered and manipulations of the subject or the subject's environment that are performed for research purposes.

(2) *Interaction* includes communication or interpersonal contact between investigator and subject.

(3) *Private information* includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator associated with the information) in order for obtaining the information to constitute research involving human subjects.

See 15 C.F.R. § 27.102 (Definitions).

1) **Requirement for Federalwide Assurance.** If the application is accepted for [or awarded] funding, organizations that have an Institutional Review Board (IRB) are required to follow the procedures of their organization for approval of exempt and non-exempt research activities that involve human subjects. Both domestic and foreign organizations performing non-exempt research activities involving human subjects will be required to have protocols approved by a cognizant, active IRB currently registered with the Office for Human Research Protections (OHRP) within the DHHS that is linked to the engaged organizations. All

engaged organizations must possess a currently valid Federalwide Assurance (FWA) on file from OHRP. Information regarding how to apply for an FWA and register an IRB with OHRP can be found at http://www.hhs.gov/ohrp/assurances/index.html. NIST relies only on OHRP-issued FWAs and IRB Registrations for both domestic and foreign organizations for NIST supported research involving human subjects. NIST will not issue its own FWAs or IRB Registrations for domestic or foreign organizations.

2) **Administrative Review.** The NIST Human Subjects Protection Office (HSPO) reserves the right to conduct an administrative review[15] of all applications that potentially include research involving human subjects and were approved by an authorized non-NIST institutional entity (an IRB or entity analogous to the NIST HSPO) under 15 C.F.R. § 27.112 (Review by Institution). If the NIST HSPO determines that an application includes research activities that potentially involve human subjects, the applicant will be required to provide additional information to NIST for review and approval. The documents required for funded proposals are listed in each section below. Most documents will need to be produced during the proposal review process; however, the Grants Officer may allow final versions of certain required documents to be produced at an appropriate designated time post-award. Research involving human subjects may not start until the NIST Grants Officer issues an award explicitly authorizing such research. In addition, all amendments, modifications, or changes to approved research and requests for continuing review and closure will be reviewed by the NIST HSPO.

3) **Required documents for proposal review. All applications involving human subject research must clearly indicate, by separable task, all research activities believed to be exempt or non-exempt research involving human subjects, the expected institution(s) where the research activities involving human subjects may be conducted, and the institution(s) expected to be engaged in the research activities.**

   a. **Not research determination.** If an activity/task involves human subjects as defined in the Common Rule, but the applicant participant(s) indicates to NIST that the activity/task is not research as defined in the Common Rule, the following information may be requested for that activity/task:

[15] Conducting an "administrative review" means that the NIST HSPO will review and verify the performing institution's determination for research not involving human subjects or exempt human subjects research. In addition, for non-exempt human subjects research, the NIST HSPO will review and confirm that the research and performing institution(s) are in compliance with 15 C.F.R. Part 27, which means HSPO will 1) confirm the engaged institution(s) possess, or are covered under a Federalwide Assurance, 2) review the research study documentation submitted to the IRB and verify the IRB's determination of level of risk and approval of the study for compliance with 15 C.F.R. Part 27, 3) review and verify IRB-approved substantive changes to an approved research study before the changes are implemented, and 4) review and verify that the IRB conducts an appropriate continuing review at least annually.

(1) Justification, including the rationale for the determination and such additional documentation as may be deemed necessary by NIST to review and/or support a determination that the activity/task in the application is not research as defined in the Common Rule.
(2) If the applicant participant(s) used a cognizant IRB that provided a determination that the activity/task is not research, a copy of that determination documentation must be provided to NIST. The applicant participant(s) is not required to establish a relationship with a cognizant IRB if they do not have one.

NIST will review the information submitted and may coordinate further with the applicant before determining whether the activity/task will be defined as research under the Common Rule in the applicable NIST financial assistance program or project.

b. **Research not involving human subjects**. If an activity/task is determined to be research and involves human subjects, but is determined to be *not human subjects research* (or *research not involving human subjects*) under the Common Rule, the following information may be requested for that activity/task:

(1) Justification, including the rationale for the determination and such additional documentation as may be deemed necessary by NIST to review and/or support a determination that the activity/task in the application is not research as defined in the Common Rule.
(2) If the applicant participant(s) used a cognizant IRB that provided a determination that the activity/task is research not involving human subjects, a copy of that determination documentation must be provided to NIST. The applicant participant(s) is not required to establish a relationship with a cognizant IRB if they do not have one.

c. **Exempt research determination with no IRB.** If the application appears to NIST to include exempt research activities, and the performer of the activity or the supplier and/or the receiver of the biological materials or data from human subjects **does not** have a cognizant IRB to provide an exemption determination, the following information may be requested during the review process so that NIST can evaluate whether an exemption under the Common Rule applies (*see* 15 C.F.R. § 27.101(b), (c) and (d)):

(1) The name(s) of the institution(s) where the exempt research will be conducted.
(2) The name(s) of the institution(s) providing the biological materials or data from human subjects.
(3) A copy of the protocol for the research to be conducted; and/or the biological materials or data from human subjects to be collected/provided, not pre-existing samples (*i.e.,* will proposed research collect only

information without personal identifiable information, will biological materials or data be de-identified and when and by whom was the de-identification performed, how were the materials or data originally collected).

(4) For pre-existing biological materials or data from human subjects, provide copies of the consent forms used for collection and a description of how the materials or data were originally collected and stripped of personal identifiers. If copies of consent forms are not available, explain.

(5) Any additional clarifying documentation that NIST may deem necessary in order to make a determination whether the activity/task or use of biological materials or data from human subjects is exempt under the Common Rule.

d. **Research review with an IRB.** If the application appears to NIST to include research activities (exempt or non-exempt) involving human subjects, and the proposed performer of the activity has a cognizant IRB registered with OHRP, and linked to their Federalwide Assurance, the following information may be requested during the review process:

(1) The name(s) of the institution(s) where the research will be conducted.
(2) The name(s) and institution(s) of the cognizant IRB(s), and the IRB registration number(s).
(3) The FWA number of the applicant linked to the cognizant IRB(s);
(4) The FWAs associated with all organizations engaged in the planned research activity/task, linked to the cognizant IRB.
(5) If the IRB review(s) is pending, the estimated start date for research involving human subjects.
(6) The IRB approval date (if currently approved for exempt or non-exempt research).
(7) If any of the engaged organizations has applied for or will apply for an FWA or IRB registration, those details should be clearly provided for each engaged organization.

If the application includes research activities involving human subjects to be performed in the first year of an award, additional documentation may be requested by NIST during pre-award review for those performers, and may include the following for those research activities:

(1) A signed (by the study principal investigator) copy of each applicable final IRB-approved protocol.
(2) A signed and dated approval letter from the cognizant IRB(s) that includes the name of the institution housing each applicable IRB, provides the start and end dates for the approval of the research activities, and any IRB-required interim reporting or continuing review requirements.

(3) A copy of any IRB-required application information, such as documentation of approval of special clearances (*i.e.,* biohazard, HIPAA, etc.) conflict-of-interest letters, or special training requirements.
(4) A brief description of what portions of the IRB submitted protocol are specifically included in the application submitted to NIST, if the protocol includes tasks not included in the application, or if the protocol is supported by multiple funding sources. For protocols with multiple funding sources, NIST will not approve the study without a non-duplication-of-funding letter indicating that no other federal funds will be used to support the tasks proposed under the proposed research or ongoing project
(5) If a new protocol will only be submitted to an IRB if an award from NIST is issued, a draft of the proposed protocol.
(6) Any additional clarifying documentation that NIST may request during the review process to perform the NIST administrative review of research involving human subjects. (*See* 15 C.F.R. § 27.112 (Review by Institution)).

This clause reflects the existing NIST policy and requirements for Research Involving Human Subjects. Should the policy be revised prior to award, a clause reflecting the policy current at time of award may be incorporated into the award.

If the policy is revised after award, a clause reflecting the updated policy may be incorporated into the award.

For more information regarding research projects involving human subjects, contact Anne Andrews, Director, NIST Human Subjects Protection Office (e-mail: anne.andrews@nist.gov; phone: (301) 975-5445).

h) Research Activities Involving Live Vertebrate Animals. Any application that includes research activities involving live vertebrate animals, that are being cared for, euthanized, or used by participants in the application to accomplish research goals, teaching, or testing, must meet the requirements of the *Animal Welfare Act* (AWA) (7 U.S.C. § 2131 et seq.), and the AWA final rules (9 C.F.R. Parts 1, 2, and 3), and if appropriate, the *Good Laboratory Practice for Non-clinical Laboratory Studies* (21 C.F.R. Part 58). In addition, such applications should be in compliance with the *U.S. Government Principles for Utilization and Care of Vertebrate Animals Used in Testing, Research, and Training*. The Principles and guidance on these Principles are available in the National Research Council's *Guide for the Care and Use of Laboratory Animals*, which can be obtained from National Academy Press, 500 5th Street, N.W., Department 285, Washington, DC 20055, or as a free PDF online at http://www.nap.edu/catalog/12910/guide-for-the-care-and-use-of-laboratory-animals-eighth.

(1) Administrative Review. NIST reserves the right to conduct an administrative review of the applicant's research activities that involve live vertebrate animals, or custom samples from, or field studies with live vertebrate animals. If the

application includes research activities, field studies, or custom samples involving live vertebrate animals, the applicant will be required to provide additional information for review and approval. In addition, NIST will verify the applicant's determination(s) of excluded samples from vertebrate animals. The documents required for funded proposals are listed in each section below. Some may be requested for a pre-review during the proposal review process; however, the Grants Officer may allow final versions of certain required documents to be produced at an appropriate designated time post-award. If an award is issued, no research activities involving live vertebrate animals shall be initiated or costs incurred for those activities under the award until the NIST Grants Officer issues written approval. In addition, all re-approvals, amendments, modifications, changes, annual reports and closure will be reviewed by NIST.

(2) Required documents for NIST proposal review. *The applicant should clearly indicate in the application, by separable task, all research activities believed to include research involving live vertebrate animals and the institution(s) where the research activities involving live vertebrate animals may be conducted. In addition, the applicant should indicate any activity/task that involves an excluded or custom collection from vertebrate animals, or a field study with animals.*

(a) Excluded Collections from Vertebrate Animals: The requirements for review and approval by an Institutional Animal Care and Use Committee (IACUC) do not apply to proposed research using preexisting images of animals or to research plans that do not include live animals. These regulations also do not apply to obtaining stock or pre-existing items from animal material suppliers (e.g. tissue banks), such as pre-existing cell lines and tissue samples, or from commercial food processors, where the vertebrate animal was euthanized for food purposes and not for the purpose of sample collection.

For pre-existing cell lines and tissue samples originating from vertebrate animals, NIST requires that the proposer provide documentation or the rationale for the determination that the cell line or tissue is pre-existing and not a custom collection from live vertebrate animals for an activity/task within the proposal. NIST may require additional documentation to review and/or support the determination that the cells and/or tissues from vertebrate animals are excluded from IACUC review.

(b) Custom Collections Harvested from Live Vertebrate Animals: NIST requires documentation for obtaining custom samples from live vertebrate animals from animal material suppliers and other organizations (i.e., universities, companies, and government laboratories, etc.). Custom samples includes samples from animal material suppliers, such as when a catalog item indicates that the researcher is to specify the characteristics of the live vertebrate animal to be used, or how a sample is to be collected from the live vertebrate animal.

(c) Field Studies of Animals: Some field studies of animals may be exempt under the Animal Welfare Act from full review and approval by an animal care and use committee, as determined by each institution. Field study is defined as "…a study conducted on free-living wild animals in their natural habitat." However, this term excludes any study that involves an invasive procedure or that harms or materially alters the behavior of an animal under study. Field studies, with or without invasive procedures, may also require obtaining appropriate federal or local government permits (e.g. marine mammals, endangered species, etc.). If the applicant's institution requires review and approval by an animal care and use committee, NIST will require that documentation to be provided as described below.

(d) For custom collections or studies with live vertebrate animals that require review and approval by an animal care and use committee the following documentation is required:

(1) Requirement for Assurance. An applicable assurance for the care and use of the live vertebrate animal(s) to be used in the proposed research is required. NIST accepts three types of assurances, as may be applicable. NIST may request documentation to confirm an assurance, if adequate confirmation is not available through an assuring organization's website. The cognizant Institutional Animal Care and Use Committee (IACUC) where the research activity is located may hold one or more applicable assurances applicable to the research activity that are acceptable to NIST. These three assurances are:

- Animal Welfare Assurance from the Office of Laboratory Animal Welfare (OLAW) indicated by the OLAW assurance number, i.e., A-1234;
- USDA Animal Welfare Act certification indicated by the certification number, i.e., 12-R-3456;
- Association for the Assessment and Accreditation of Laboratory Animal Care (AAALAC) indicated by providing the organization name accredited by AAALAC as listed in the AAALAC Directory of Accredited Organizations.

(2) Documentation of Research Review by an IACUC: If the applicant's application appears to include research activities, field studies, or custom sample collections involving live vertebrate animals the following information regarding review by an applicable IACUC may be requested during the application review process:

- The name(s) of the institution(s) where the research involving live vertebrate animals will be conducted and/or custom samples collected;

- The assurance type and number, as applicable, for the cognizant Institutional Animal Care and Use Committee (IACUC) where the research activity is located. [For example: Animal Welfare Assurance from the Office of Laboratory Animal Welfare (OLAW) should be indicated by the OLAW assurance number, i.e. A-1234; an USDA Animal Welfare Act certification should be indicated by the certification number i.e. 12-R-3456; and an Association for the Assessment and Accreditation of Laboratory Animal Care (AAALAC) should be indicated by AAALAC.]
- The IACUC approval date for the Animal Study Protocol (ASP) (if currently approved);
- If the review by the cognizant IACUC is pending, the estimated- start date for research involving vertebrate animals;
- If any assurances or IACUCs need to be obtained or established, that should be clearly stated.
- If any special permits are required for field studies, those details should be clearly provided for each instance, or indicated as pending.

If the application includes research activities involving vertebrate animals to be performed in the first year of an award, additional documentation may be requested by NIST during pre-award review for those performers, and may include the following for those research activities, to include field studies and custom sample collections involving live vertebrate animals:

(a) A copy of the IACUC approved ASP signed by the Principal Investigator;
(b) Documentation of the IACUC approval indicating the approval and expiration dates of the ASP; and
(c) If applicable, a non-duplication-of-funding letter if the ASP is funded from several sources.
(d) If a new ASP will only be submitted to an IACUC if an award from NIST is issued, a draft of the proposed ASP may be requested.
(e) Any additional clarifying documentation that NIST may request during review of applications to perform the NIST administrative review of research involving live vertebrate animals.

This clause reflects the existing NIST policy for Research Involving Live Vertebrate Animals. Should the policy be revised prior to award, a clause reflecting the policy current at time of award may be incorporated into the award.

If the policy is revised after award, a clause reflecting the updated policy may be incorporated into the award.

For more information regarding research projects involving live vertebrate animals, contact Linda Beth Schilling, Senior Analyst (linda.schilling@nist.gov; 301-975-2887).

3. Reporting

a) Reporting Requirements. The following reporting requirements described in Sections A.01 Performance (Technical) Reports and B.02 Financial Reports of the DoC Financial Assistance Standard Terms and Conditions dated December 26, 2014, http://go.usa.gov/hKbj apply to awards in this program:

(1) Financial Reports. Each award recipient will be required to submit an SF-425, Federal Financial Report on a quarterly basis for the periods ending March 31, June 30, September 30, and December 31 of each year. Reports will be due within 30 days after the end of the reporting period to the NIST Grants Officer and Grants Specialist named in the award documents. A final financial report is due within 90 days after the end of the project period.

(2) Performance (Technical) Reports. Each award recipient will be required to submit a technical progress report to the NIST Grants Officer and the NIST Federal Program Officer on a quarterly basis for the periods ending March 31, June 30, September 30, and December 31 of each year. Reports will be due within 30 days after the end of the reporting period. A final technical progress report shall be submitted within 90 days after the expiration date of the award. Technical progress reports shall conform to the requirements in 2 C.F.R. § 200.328 (http://go.usa.gov/xkVgP) and Department of Commerce Standard Terms and Conditions, Section A.01 (http://go.usa.gov/hKbj).

(3) Patent and Property Reports. From time to time, and in accordance with the Uniform Administrative Requirements (*see* Section VI.2 of this NOFO) and other terms and conditions governing the award, the recipient may need to submit property and patent reports.

(4) Recipient Integrity and Performance Matters. In accordance with section 872 of Public Law 110-417 (as amended; see 41 U.S.C. 2313), if the total value of a recipient's currently active grants, cooperative agreements, and procurement contracts from all Federal awarding agencies exceeds $10,000,000 for any period of time during the period of performance of an award made under this NOFO, then the recipient shall be subject to the requirements specified in Appendix XII to 2 C.F.R. Part 200, http://go.usa.gov/cTBwC, for maintaining the currency of information reported to SAM that is made available in FAPIIS about certain civil, criminal, or administrative proceedings involving the recipient.

b) Audit Requirements. 2 C.F.R. Subpart F, adopted by the Department of Commerce through 2 C.F.R. § 1327.101 requires any non-Federal entity (i.e., including non-profit institutions of higher education and other non-profit organizations) that expends Federal awards of $750,000 or more in the recipient's fiscal year to conduct a single or program-specific audit in accordance with the requirements set out in the Subpart. Applicants are reminded that NIST, the DoC Office of Inspector General, or another authorized Federal agency may conduct an audit of an award at any time.

c) **Federal Funding Accountability and Transparency Act of 2006.** In accordance with 2 C.F.R. Part 170, all recipients of a Federal award made on or after October 1, 2010, are required to comply with reporting requirements under the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No. 109-282). In general, all recipients are responsible for reporting sub-awards of $25,000 or more. In addition, recipients that meet certain criteria are responsible for reporting executive compensation. Applicants must ensure they have the necessary processes and systems in place to comply with the reporting requirements should they receive funding. Also see the Federal Register notice published September 14, 2010, at 75 FR 55663 available here http://go.usa.gov/hKnQ.

4. Award Management and Public Engagement

Publication and Technology Transfer. Each award recipient is expected to present the results of their work in appropriate professional literature and conferences in order to make the findings broadly available. Data supporting any findings or conclusions shall be made available in a manner consistent with the Data Management Plan.

VII. Federal Awarding Agency Contacts

Questions should be directed to the following:

Subject Area	Point of Contact
Programmatic and Technical Questions	E-mail: pscr@nist.gov
Technical Assistance with Grants.gov Submissions	Christopher Hunton Phone: 301-975-5718 Fax: 301-975-8884 E-mail: grants@nist.gov Or www.grants.gov Phone: 800-518-4726 E-mail: support@grants.gov
Grant Rules and Regulations	Scott McNichol Phone: 303-497-3444 Fax: 303-497-5470 E-mail: scott.mcnichol@nist.gov

VIII. Other Information

1. Protected and Proprietary Information

The applicant acknowledges and understands that information and data contained in applications for financial assistance, as well as information and data contained in financial, performance and other reports submitted by applicants, may be used by the Department of Commerce in conducting reviews and evaluations of its financial assistance programs. For this purpose, applicant information and data may be accessed, reviewed and evaluated by Department of Commerce employees, other Federal employees, Federal agents and contractors, and/or by non-Federal personnel, all of whom enter into appropriate conflicts of interest and nondisclosure agreements covering the use of such information. As may be provided in the terms and conditions of a specific financial assistance award, applicants are expected to support program reviews and evaluations by submitting required financial and performance information and data in an accurate and timely manner, and by cooperating with Department of Commerce and external program evaluators. In accordance with 2 C.F.R. § 200.303(e), applicants are reminded that they must take reasonable measures to safeguard protected personally identifiable information and other confidential or sensitive personal or business information created or obtained in connection with a Department of Commerce financial assistance award.

In addition, Department of Commerce regulations implementing the Freedom of Information Act (FOIA), 5 U.S.C. Sec. 552, are found at 15 C.F.R. Part 4, Public Information. These regulations set forth rules for the Department regarding making requested materials, information, and records publicly available under the FOIA. Applications submitted in response to this Federal Funding Opportunity may be subject to requests for release under the Act. In the event that an application contains information or data that the applicant deems to be confidential commercial information that should be exempt from disclosure under FOIA, that information should be identified, bracketed, and marked as Privileged, Confidential, Commercial or Financial Information. In accordance with 15 CFR § 4.9, the Department of Commerce will protect from disclosure confidential business information contained in financial assistance applications and other documentation provided by applicants to the extent permitted by law.

2. Public Website, Frequently Asked Questions (FAQS) and Webinar

NIST has a public website (https://www.nist.gov/ctl/pscr) that provides information pertaining to this Funding Opportunity[16]. NIST anticipates that a “Frequently Asked Questions” section or other resource materials will be maintained and updated on the website as needed to provide additional guidance and clarifying information that may arise related to this Funding Opportunity. Any amendments to this NOFO will be announced through Grants.gov.

[16] Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Programmatic and Technical Questions, if this link is no longer working or more information is needed.

Applicants must submit all questions pertaining to this funding opportunity in writing to pscr@nist.gov. Questions submitted to NIST may be posted on https://www.nist.gov/ctl/pscr. Alternatively, applicants may ask questions during the informational public webinar as described in the next paragraph.

NIST will host a webinar to provide general information regarding this NOFO, offer general guidance on preparing applications, and answer questions. Scheduling details about the webinar will be available at www.nist.gov/ctl/pscr. Proprietary technical discussions about specific project ideas will not be permitted and NIST staff will not critique or provide feedback on specific project ideas while they are being developed by an applicant or brought forth during the webinar or at any time before the deadline for all applications. However, questions about the PSIAP, eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application can be addressed at the webinar and by e-mail to pscr@nist.gov as described in the previous paragraph. There is no cost to attend the webinar, but participants must register in advance. Participation in the webinar is not required, and will not be considered in the application review and selection process. Additional information on the PSIAP and webinar is available at https://www.nist.gov/ctl/pscr.