Friday, December 18, 2015

ANNOUNCEMENT OF FEDERAL FUNDING OPPORTUNITY (FFO)
National Strategy for Trusted Identities in Cyberspace (NSTIC)
State Pilots Cooperative Agreement Program

EXECUTIVE SUMMARY

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

- **Funding Opportunity Title:** National Strategy for Trusted Identities in Cyberspace (NSTIC) State Pilots Cooperative Agreement Program

- **Announcement Type:** Initial

- **Funding Opportunity Number:** 2016-NIST-NSTIC-01

- **Catalog of Federal Domestic Assistance (CFDA) Number:** 11.619, Arrangements for Interdisciplinary Research Infrastructure

- **Dates:** Abbreviated Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, Thursday, February 18, 2016. Abbreviated 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 at these times: from 12:01 a.m. Eastern Time, Saturday, January 16, 2016 until Tuesday, January 19, 2016, at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, February 20, 2016 until Monday, February 22, 2016 at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, April 16, 2016 until Monday, April 18, 2016 at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, May 21, 2016 until Monday, May 23, 2016 at 6:00 a.m. Eastern Time. Applications cannot be submitted when Grants.gov is closed.** NIST expects to complete its review of Abbreviated Applications and selection of finalists by Friday, March 25, 2016. Full Applications must be received electronically at Grants.gov no later than 11:59 p.m. Eastern Time, Wednesday, May 25, 2016. Full Applications received after this deadline will not be reviewed or considered. Full Applications received from applicants who were not invited to submit a Full Application will not be reviewed or considered. NIST expects to complete its review of Full Applications, selection of successful applicants, and award processing in August 2016. NIST expects the earliest anticipated start date for awards under this FFO to be September 1, 2016.

  When developing your submission timeline, please keep in mind that (1) all applicants are required to have a current registration in the System for Award Management (SAM.gov); (2) the free annual registration process in the electronic

System for Award Management (SAM.gov) (*see* Section IV.3. and Section IV.7.a.(1).b. of this FFO) may take between three and five business days or as long as more than two weeks; and (3) electronic applicants are required to have a current registration in Grants.gov; and (4) applicants using Grants.gov 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. 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:** NIST is soliciting applications from eligible applicants to pilot online identity solutions that embrace the Identity Ecosystem Steering Group's (IDESG) Identity Ecosystem Framework (IDEF).[1] Specifically, identity solutions must:

  1. Enable online access to one or more state, local, or tribal government service(s).
  2. Provide for a federated, verified digital identity that enables multi-factor authentication and an effective identity proofing process meeting the risk needs of the service(s).
  3. Aligns with the Identity Ecosystem Framework Requirements.
  4. Allow for interoperability with other federations in use in the public and private sectors.

NIST encourages pilots that maximize their contribution to the ongoing development and adoption of the Identity Ecosystem Framework, the OpenID Foundation iGov Working Group, and other public fora.

.

- **Anticipated Amounts:** NIST anticipates funding up to four (4) awards; each award will be in the range of approximately $1,000,000 to $1,250,000 per year for up to three years, consistent with the multi-year funding policy described in Section II.2. of this FFO. NIST will consider applications that propose lower funding amounts. NIST anticipates funding new pilots with total FY2016 funding of up to approximately $4 million.

- **Funding Instrument:** Cooperative agreement.

- **Who Is Eligible:** All applicants must meet one of the following conditions to be eligible:

[1] https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents

- State, local, or Indian tribal governments located in the United States and its territories, or
- Commercial or nonprofit organizations or institutions of higher education located in the United States that have at least two state, local, or tribal government agencies representing two different governmental jurisdictions participating in the pilot through enabling online access to one or more state, local, or tribal government service(s)**.**

Federal agencies may participate in projects but may not receive NIST funding.

- **Cost Sharing Requirements:** This program does not require cost sharing.

- **Public Meetings (Applicants' Conference):** NIST will hold a webinar (Applicants' Conference) to provide general information regarding the NSTIC, to offer general guidance on preparing applications, and to answer questions. Proprietary technical discussions about specific project ideas with NIST staff are not permitted at this conference or at any time before submitting an application to NIST. Therefore, applicants should not expect to have proprietary issues addressed at the Applicants' Conference. Also, NIST/NSTIC Program Office staff will not critique or provide feedback on specific project ideas while they are being developed by an applicant. However, NIST/NSTIC Program Office staff will answer questions about the National Strategy for Trusted Identities in Cyberspace (NSTIC) State Pilots Cooperative Agreement Program (NSTIC State Pilots Cooperative Agreement Program) eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application at the Applicants' Conference and by phone and email. Attendance at the Applicants' Conference is not required. Information on the Applicants' Conference is available at http://www.nist.gov/nstic/funding-opportunities.html.

Table of Contents

I. Program Description..... 4

II. Federal Award Information..... 7

III. Eligibility Information 8

IV. Application Submission Information..... 8

V. Application Review Information..... 22

VI. Federal Award Administration Information 29

VII. Federal Awarding Agency Contact(s) 37

VIII. Other Information..... 38

FULL ANNOUNCEMENT TEXT

I. Program Description

The statutory authority for the National Strategy for Trusted Identities in Cyberspace (NSTIC) State Pilots Cooperative Agreement Program is 15 U.S.C. §§ 272(b)(1), (b)(4), (c)(12), and (c)(14).

In April 2011, President Obama signed the National Strategy for Trusted Identities in Cyberspace (NSTIC or Strategy), which charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions. The Strategy can be found at: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

The Strategy envisions a user-centric Identity Ecosystem, defined as "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices."[2]

NSTIC specifies four guiding principles to which the Identity Ecosystem must adhere:

1. Identity solutions will be privacy-enhancing and voluntary;
2. Identity solutions will be secure and resilient;
3. Identity solutions will be interoperable; and
4. Identity solutions will be cost-effective and easy to use.

The Strategy will only be a success – and the ideal of the Identity Ecosystem will only be achieved – if identity solutions fulfill all of these guiding principles. Achieving them separately will not only lead to an inadequate solution but could serve as a hindrance to the broader evolution of cyberspace.

The Strategy emphasizes that some parts of the Identity Ecosystem exist today but recognizes that there is still much work to be done. NIST has established a National Program Office (NPO) to lead the implementation of NSTIC, with a focus on promoting private sector involvement and engagement; supporting interagency collaboration and coordinating interagency efforts associated with achieving programmatic goals; building consensus on policy frameworks necessary to achieve the vision; identifying areas for the government to lead by example in developing and supporting the Identity Ecosystem, particularly in the Executive Branch's role as a provider and validator of key credentials and attributes; actively participating within and across relevant public-

[2] National Strategy for Trusted Identities in Cyberspace at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf, p. 2

and private-sector forums; and assessing progress against the goals, objectives, and milestones of the NSTIC.

More information about the NSTIC NPO is available at http://www.nist.gov/nstic/.

NIST Funded Projects Advancing the NSTIC Strategy

In implementing the Strategy, the NSTIC NPO seeks to build upon the existing marketplace, encourage new solutions, and establish a baseline of privacy, security, interoperability, and ease-of-use of trusted digital identity credentials that will improve trust in online transactions while enabling the market in online credentials to flourish.

NIST began funding pilot projects under the NSTIC Pilots Cooperative Agreement Program in 2012 and has made awards for pilot projects in each of the subsequent years. Descriptions of the pilot projects funded in the past are available on the NSTIC website at http://www.nist.gov/nstic/pilot-projects.html. As the role of online identity evolves, the NSTIC NPO is transitioning the Pilots Cooperative Agreement Program to fill more critical gaps in the Identity Ecosystem; for example, the NPO released a solicitation in 2015 specifically focused on advancing privacy-enhancing technologies, the first NPO effort to dedicate funding to a single aspect of identity solutions. The current funding opportunity continues this transition as the NSTIC NPO seeks to target specific impediments to the market through a more diverse set of opportunities.

To further advance the development of the Identity Ecosystem Framework and to build on the existing marketplace in online credentials, NIST has provided financial assistance to the Identity Ecosystem Steering Group (IDESG). The IDESG is the only private sector organization currently committed to managing the development of the Identity Ecosystem Framework. More information on the IDESG is available at http://www.idecosystem.org.

State Pilots Program Focus Area: Digitally Delivering Trustworthy Constituent Services

The purpose of the NSTIC State Pilots Cooperative Agreement Program is to pilot online identity solutions that embrace and advance the NSTIC vision of an Identity Ecosystem. Specifically, identity solutions must:

1. Enable online access to one or more state, local, or tribal government service(s).
2. Provide for a federated, verified identity that enables multi-factor authentication and an effective identity proofing process meeting the risk needs of the service(s).
3. Align with the Identity Ecosystem Framework Requirements.
4. Allow for interoperability with other federations in use in the public and private sectors.

Pilots are encouraged to maximize their contribution to the ongoing development and adoption of the Identity Ecosystem Framework, the OpenID Foundation iGov Working Group, and other public fora.

NIST will fund projects that will introduce innovative solutions that would otherwise not occur in the marketplace, for instance, projects that will deploy pilots to test or demonstrate new solutions that are not widely adopted today. The NSTIC NPO defines pilots as systems deployed in production environments that include real users conducting real transactions with real data. The pilot system may be segregated legally or technically from the operations of a full production system.

The NSTIC NPO envisions the pilots as key contributors to the ongoing development of the Identity Ecosystem Framework. The NSTIC pilots provide examples of real world achievements addressing identity-related challenges.

Many past efforts to enable the use of strong online credentials for access to government services have encountered a number of barriers, including:

1. Concerns about applicant and beneficiary privacy, including risks that arise from the crossing of contextual boundaries (e.g., risks to privacy created by entities in different sectors linking individuals' transactions) and the capacity for more tracking and profiling of individuals.

2. Difficulties conducting effective identity proofing and ensuring that selected identity proofing approaches cover the full beneficiary population.

3. Concerns that the identity management process may place additional burdens on the target audience and increase barriers to accessing state services.

4. Lack of implementation of alternative identity proofing methods beyond those that rely solely on knowledge-based schemes.

5. Balancing transparency to individual users and ease-of-use especially of strong authentication technologies.

Specifically, the NSTIC NPO is interested in funding projects with innovative approaches that overcome these barriers and advance NSTIC's four guiding principles. Because these barriers work in concert with each other, the NSTIC NPO anticipates that the best projects will address most or all of them. By doing so, the projects can provide a foundation for improving identity verification for, and increasing the efficiency of, government services.

Priority will be given to projects that demonstrate the potential for interoperability of identity credentials issued in partnership with a private provider with both state and Federal programs. The goal is to encourage partnerships between private sector providers and governments at all levels.

While the solutions may be vendor-supplied proprietary solutions, NIST requires that the solutions be interoperable within the Identity Ecosystem and not preclude integration with other public or private sector federations. The pilots must demonstrate that the approach could be replicated across multiple agencies, programs, and jurisdictions.

To further demonstrate the benefits of the solutions to both the government agencies involved and the individual users, NIST will be contracting for an independent evaluation of projects funded under this program for the efficacy of the approach in facilitating constituent access to government programs and services.

Project participants (the project lead, contractors, subawardees and other collaborators) must demonstrate that they have the education, experience, and training to pursue and advance implementation of the NSTIC. Project participants should demonstrate the strength of the partnership and highlight any prior collaborations among the participants.

II. Federal Award Information

1. **Funding Instrument.** The funding instrument that will be used is a cooperative agreement. The nature of NIST's "substantial involvement" is described in Chapter 5.C of the Department of Commerce (DoC) Grants and Cooperative Agreements Manual, which is available at http://go.usa.gov/SNJd. Please note the Department of Commerce Grants and Cooperative Agreements Manual is expected to be updated after publication of this funding announcement and before awards are made under this FFO. Refer to Section VII. of this FFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if you seek the information at this link and it is no longer working or you need more information.

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 for that award beyond the initial obligation. 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 NIST, and the availability of funds.

3. **Funding Availability.** NIST anticipates funding up to four (4) awards; each award will be in the range of approximately $1,000,000 to $1,250,000 per year per project for up to three years, consistent with the multi-year funding policy described in Section II.2. of this FFO. Proposed funding levels must be consistent with project scope. NIST will consider applications that propose lower funding amounts. NIST

anticipates funding new pilots with total FY2016 funding of up to approximately $4 million.

III. Eligibility Information

1. Eligible Applicants. All applicants must meet one of the following conditions to be eligible:

- State, local, or Indian tribal governments located in the United States and its territories, or
- Commercial or nonprofit organizations or universities located in the United States that have at least two state, local or tribal government agencies from two different governmental jurisdictions participating in the pilot.

Federal agencies may participate in projects but may not receive NIST funding.

2. Cost Sharing or Matching. This program does not require cost sharing.

IV. Application Submission Information

1. Address to Request Application Package. The application package for the Abbreviated Application is available at www.grants.gov under Funding Opportunity Number 2016-NIST-NSTIC-01. The instructions for retrieving the Full Application package from the Grants.gov website will be sent only to those invited to submit Full Applications.

2. Content and Format of Application Submission

a. Required Abbreviated Application Form and Documents

As described in Section IV.2.b., NIST requires Abbreviated Applications under the NSTIC State Pilots Cooperative Agreement Program, and the Selecting Official will select finalists from among the Abbreviated Applications. Only those applicants whose Abbreviated Applications are selected as finalists will be invited to submit Full Applications.

The Abbreviated Applications must be received electronically at Grants.gov in order to be considered for funding. The Abbreviated 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, must list the FFO number 2016-NIST-NSTIC-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) Abbreviated Proposal. Maximum four (4) page document describing the proposed project that includes sufficient information to determine that the project is within the scope of this funding opportunity and explains how the identity solution will:

a. Provide for a federated, verified identity that enables multi-factor authentication that meets the risk needs of the service(s);
b. Provide for an effective identity proofing process that meets the risk needs of the service(s);
c. Show alignment to the Identity Ecosystem Framework requirements;
d. Enable online access to at least two state, local, or tribal government services; and
e. Allow for interoperability with other federations in use in the public and private sectors.

(3) For applications led by non-governmental entities, Letters of Interest. To demonstrate that the required two state, local or tribal governmental entities are involved in the project, the applicant must attach letters of interest from each entity interested in participating in the project.

Item IV.2.a.(1) above is part of the standard application package in Grants.gov and can be completed through the download application process. **Items IV.2.a.(2) and IV.2.a.(3) must be completed and attached by clicking on the "Add Attachments" button found in Item 15 of the SF-424. 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 does not provide details concerning whether all attachments (or how many attachments) transferred successfully.** 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.

b. Required Full Application Forms and Documents

Only applicants whose Abbreviated Applications have been selected by NIST as "finalists" and who have been invited to submit a Full Application are

permitted to submit Full Applications to NIST for the NSTIC State Pilots Cooperative Agreement Program. NIST will not review Full Applications submitted by applicants who have not been selected as finalists or those submitted by applicants who did not submit an Abbreviated Application. The Full 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 FFO number provided in the special application instructions.

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 each year of the project of no more than three years, considering all potential cost increases, including cost of living adjustments.

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

(4) **CD-511, Certification Regarding Lobbying**

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

(6) **Technical Proposal.** The Technical Proposal is a document of no more than twenty-five (25) pages responsive to the program description (*see* Section I. of this FFO) and the evaluation criteria (*see* Section V.1. of this FFO). Applicants should include in their proposal a clear statement whether it is addressing all barriers to the emerging identity ecosystem, detailing how it will address those barriers, and providing clear, measurable performance objectives that can be used to determine the success of the proposed pilot project. If any barriers are not addressed, explain why addressing that specific barrier is not necessary to the pilot. Examples of clear, measurable success metrics include the expected number of users per pilot, false acceptance rates, false rejection rates, etc. The Technical Proposal should contain the following information:

(a) Executive Summary. An executive summary of the proposed project, including referencing the barriers to the Identity Ecosystem addressed, the use cases to be piloted, and the identity solution. If the application does not address all barriers from Section I, the applicant should explain

why the omitted barriers are not applicable to the pilot. The executive summary should include information indicating how each evaluation criterion and its sub-factors are addressed. A table may be helpful in providing this information.

(b) Problem Statement and Use Cases. A problem statement that discusses the specific use cases to be piloted including the specific benefit programs and characteristics of the beneficiary populations, including the size. The applicant should clearly state the solution that this project would introduce to the marketplace and what would otherwise occur without the project. The applicant must provide a justification for why the problem(s) is (are) impeding the emergence of the Identity Ecosystem. This section should also provide information on any special characteristics of the benefit program including any waivers needed such as a waiver from a Federal program office allowing a state administered program to collect date of birth information from an applicant. The application should explain why those use cases were chosen. This section provides critical background for the discussion of the proposed operational pilot.

(c) Technical Architecture. A description of the technical architecture for the proposed operational pilot, sufficient to permit evaluation of the proposal in accordance with the evaluation criteria (*see* Section V.1. of this FFO). This should include information on all the components of the solution(s), how these components interconnect, and what information is exchanged among the components. An architecture diagram and data flow diagrams including data flows among project participants can be used to present this information and will not be counted within the page limit. The applicant should provide information on what needs to be done to initiate the pilot, complete the pilot, and evaluate the pilot including the number of beneficiaries, and the percentage this represents of the total potential beneficiary population, required to make the pilot successful. A mapping to the IDESG's Identity Ecosystem Framework requirements (*see* http://www.idesg.org/IdentityRevolution) will help in the evaluation.

The solution description, including any architecture and data flow diagrams, should make clear how the solution mitigates privacy and civil liberties risks arising from the capability for greater identification, tracking or linkability of transactions, and personal data aggregation. Privacy and civil liberties protections may be enforced by either (or both) technical and policy means; however, technical means for mitigating privacy risks are preferable to policy mitigations. This section should explain how the technical and policy measures are applied in a risk-based approach to address privacy concerns - for example, NIST's privacy risk model as documented in *Privacy Risk Management for Federal Information*

Systems, NISTIR 8062 *(DRAFT)* (http://csrc.nist.gov/projects/privacy_engineering/documents.html). This section should address the *Quality of the Proposed Technical Solution* evaluation criterion (*see* Section V.2.a. of this FFO).

(d) Statement of Work and Implementation Plan. A complete statement of work covering all project participants including relying parties that includes the following:

- Measurable performance objectives used to determine the success of the pilot project along with the required metrics to indicate success;
- Specific proposed tasks;
- Schedule of measurable events and realistic, measurable milestones including any state budget authorization actions required and Federal waivers required;
- The project leadership's plans to manage all project participants, including sub-recipients, contractors, etc., to ensure realization of project goals and objectives; and
- Approach to ensure the project results will align to the IDESG's IDEF.

All aspects discussed as part of the solution should be included in the implementation plan and have associated milestones with performance metrics specified. For example, milestones and metrics could include the dates of go-lives, the target number of users per pilot phase, and the maximum false accept rates. The schedule of tasks and events can be presented as a Gantt chart, work breakdown structure (WBS) or other formats. (Note that the Gantt chart, WBS, or other, similar planning documents are not counted within the page limit.)

This section should address the *Quality of the Implementation Plan* evaluation criterion (*see* Section V.1.b. of this FFO).

(e) Project Impact. A description of the plans to scale the pilot project into full production and self-sustaining, large scale use. This section should also describe the project participants' planned role(s) in organizations developing the Identity Ecosystem Framework as envisioned in the NSTIC Strategy (e.g., the committees and working groups of the IDESG). Include also any planned efforts to disseminate information and reach out to users. This section should address the *Contribution to the Identity Ecosystem* evaluation criterion (*see* Section V.1.c. of this FFO).

(f) Qualifications. A description of the qualifications, proposed roles, and level of planned effort of the project participants, including the proposed role of the project lead and of each subwardee, contractor or other collaborator, including the state, local or tribal governments participating in the project. Include past experience collaborating, if applicable.

All participating organizations are expected to identify at least one key person and that person's time commitment to the project. It is anticipated that all key personnel will participate in biweekly project status discussions with the NPO. The key personnel should include the following:

- At least one individual from each participant, with details of committed participation. It may be that multiple individuals are needed to represent all stakeholders within a participant (for example, individuals representing the relevant state IT organization and state program providing the service would likely both be needed).
- A project manager or project leader with demonstrated experience leading projects of similar size and complexity and previously demonstrated ability to achieve positive outcomes in pilot programs and similar endeavors.
- At least one privacy engineer with specialized knowledge of both privacy technology and policy issues is expected on all projects. This individual(s) will be considered key to the project and shall ideally have at least 5-7 years' experience in a cross-set of privacy and information technology skills. This individual may be an employee of the applicant, or he or she may be a consultant or employee of a contractor or subawardee. Although less preferable, this role could be filled by multiple individuals with complementary skillsets and experience. Experience may be demonstrated by education, certifications, and job skills. Qualifications for the privacy skillset could include certifications such as CIPT or CIPM and experience implementing privacy principles such as the Fair Information Practice Principles, identifying and mitigating privacy risks in the implementation of information technology systems. Qualifications for the technical skillset could include advanced degrees in computer science, information science, or computer engineering and experience with architectural design for information systems; data, systems, or software engineering; and related aspects of technical privacy implementations. If multiple individuals are used to meet this qualification, the applicant must include a description of how the multiple individuals will work together to compensate for the lack of the combined skillset in a single individual.
- At least one subject matter expert in addressing usability of the type of system envisioned for the project and the beneficiary population.

Resumes of all key personnel including the privacy engineer(s), usability expert(s), and project manager(s) are required and are not included in the page count. Resumes are to be a maximum of two (2) pages each.

This section, the budget narrative, letters of commitment and the resumes should address the *Resource Availability* evaluation criterion (*see* Section V.1.d. of this FFO).

(7) Budget Narrative. The Budget Narrative should 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). 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. Applicants can include in the budget the time to participate in forums (such as committees of the IDESG) developing elements of the Identity Ecosystem Framework as envisioned in the NSTIC strategy. The cost of the time required to prepare presentations to report on the progress of the project to the IDESG should also be included in this category.

(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 – NIST will require that award recipients report on their projects twice a year to the Identity Ecosystem Steering Group (http://www.idecosystem.org/). Therefore, applicants should include travel costs for at least two meetings of the IDESG per year and may include costs for up to four IDESG meetings per year in their budget narrative. For travel costs associated with travel to these meetings, and additional travel required by the recipient to complete the project, the budget justification for travel should include the following: destination; names/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.

(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 provided and the necessity of the subaward or contract to the successful performance of the proposed project. Contracts are for obtaining normal 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, 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.

(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 or Interest. Letters are not included in the page count.

(a) Letters of Commitment to participate. If the project is not led by a state, local, or tribal government agency, letters of commitment are required from at least two state, local, or tribal government agencies from two different governmental jurisdictions.

If the application identifies other third parties including contractors, subawardees, and/or other collaborators, who will participate in the proposed project, then the applicant must provide a letter from each currently known participant describing its participation. Each letter should indicate the organization's willingness to participate, what they will be doing for the project, and the level of organizational commitment to the project. A letter is required whether or not the organization is receiving Federal funds. Note that the letters of commitment are part of the material addressing *Resource Availability* evaluation criterion (*see* Section V.1.d of this FFO).

(b) Letters of Interest, optional. Letters of interest may be provided from parties who might become customers for the solutions discussed in the proposed project.

(10) Resumes of Key Personnel including Privacy Experts. Resumes of all key personnel including the project's privacy expert(s), usability expert(s), and project manager are required. These resumes are to be a maximum of two (2) pages each. Note that the resumes are part of the material addressing *Resource Availability* evaluation criterion (*see* Section V.1.d. of this FFO).

(11) Data Management Plan. In accordance with the Office of Science and Technology Memorandum for the Heads of Executive Departments and Agencies of February 22, 2013[3], *Increasing Access to the Results of Federally Funded Scientific Research*, and as implemented through NIST Policy 5700.00[4], *Managing Public Access to Results of Federally Funded*

[3] https://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf
[4] http://www.nist.gov/open/upload/Final-P-5700.pdf

Research, and NIST Order 5701.00[5], *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 (2) 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[6] or the National Institutes of Health[7]). Some organizations' templates are available on the Internet[8].

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/or 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.4.a. of this FFO); however, the DMP will not be evaluated against any evaluation criteria.

Items IV.2.b.(1) through IV.2.b.(5) above are part of the standard application package in Grants.gov and can be completed through the download application process. **Items IV.2.b.(6) through IV.2.b.(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***

[5] http://www.nist.gov/open/upload/Final-O-5701_0.pdf
[6] http://www.nsf.gov/bfa/dias/policy/dmp.jsp
[7] http://grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm
[8] https://www.cic.net/projects/technology/shared-storage-services/data-management-plans

attachments (or how many attachments) transferred successfully. Applicants using Grants.gov 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.

The Grants.gov Online Users Guide available at the Grants.gov site (http://go.usa.gov/cjaEh) provides vital information on checking the status of applications. See especially the "Check My Application Status" option, found by clicking first on Applicants, and then by clicking on Applicant Actions.

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.

Checking the application status and tracking the submission are useful tools in the Abbreviated Application stage as well as in the Full Application stage.

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

c. Application Format

Note that these formatting requirements apply to both Abbreviated and Full Applications. Where there are differences, such differences are noted.

(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 (10-point minimum). Smaller type may be used in figures and tables but must be clearly legible.

(4) **Page Limit.** The Abbreviated Proposal for Abbreviated Applications is limited to four (4) pages, and the Technical Proposal for Full Applications is limited to twenty-five (25) pages.

(a) For Abbreviated Applications:

Page limit includes: Abbreviated Proposal addressing the criteria. This includes any figures, graphs, tables, images, and pictures.

Page limit excludes: SF-424, Application for Federal Assistance, Letters of Interest

(b) For Full Applications:

Page limit includes: Table of contents (if included), Technical Proposal with all required information, including management information and qualifications, figures, graphs, tables, images, and pictures.

Page limit excludes: SF-424, Application for Federal Assistance; SF-424A, Budget Information – Non-Construction Programs; SF-424B, Assurances – Non-Construction Programs; SF-LLL, Disclosure of Lobbying Activities; CD-511, Certification Regarding Lobbying; Cover Page; Gantt Chart, WBS, or other planning document (if included); Architecture and data flow diagrams (if included); detailed analysis of the privacy risks of the solution (e.g., an analysis against NIST's privacy risk model (see http://csrc.nist.gov/projects/privacy_engineering/documents.html); Budget Narrative; Indirect Cost Rate Agreement; Letters of Commitment or Interest; Resumes of Key Personnel including Privacy Experts; and Data Management Plan.

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

(6) Application language. English.

d. Application Replacement Pages. Applicants may not submit replacement pages and/or missing documents once an application has been submitted. Any revisions must be made by submission of a new application that must be received by NIST by the submission deadline.

e. Pre-Applications. NIST requires **Abbreviated Applications** under the NSTIC State Pilots Cooperative Agreement Program (*see* Section IV.2.a. of this FFO). The Selection Official will select from among the Abbreviated Applications a group of finalists to submit Full Applications.

f. 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 FFO, 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.** Abbreviated Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, Thursday, February 18, 2016. Abbreviated 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 at these times: from 12:01 a.m. Eastern Time, Saturday, January 16, 2016 until Tuesday, January 19, 2016, at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, February 20, 2016 until Monday, February 22, 2016 at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, April 16, 2016 until Monday, April 18, 2016 at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, May 21, 2016 until Monday, May 23, 2016 at 6:00 a.m. Eastern Time. Applications cannot be submitted when Grants.gov is closed.** Review of Abbreviated Applications and selection of finalists is expected to be completed by Friday, March 25, 2016. Full Applications must be received electronically at Grants.gov no later than 11:59 p.m. Eastern Time, Wednesday, May 25, 2016. Full Applications received after this deadline will not be reviewed or considered. Full Applications received from applicants who were not invited to submit a Full Application will not be reviewed or considered. Review of Full Applications, selection of successful applicants, and award processing is expected to be completed in August 2016. The earliest anticipated start date for awards under this FFO is expected to be September 1, 2016.

   When developing your submission timeline, please keep in mind that (1) all applicants are required to have a current registration in the System for Award Management (SAM.gov); (2) the free annual registration process in the electronic System for Award Management (SAM.gov) (*see* Section IV.3. and Section IV.7.a.(1).b. of this FFO) may take between three and five business days or as long as more than two weeks; and (3) applicants are required to have a current registration in Grants.gov; and (4) 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. 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. 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 2016-NIST-NSTIC-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 (3) to five (5) business days. If problems are encountered, the registration process can take up to two (2) 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. *See also* Section IV.3. of this FFO. 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, you 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 your 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 your application is received on time.

b. Amendments. Any amendments to this FFO will be announced through Grants.gov. Applicants may sign up on Grants.gov to receive amendments by e-mail or may request copies from Barbara Cuthill by telephone at (301) 975-3273 or by e-mail to nstic@nist.gov.

V. Application Review Information

1. Evaluation Criteria for Abbreviated Applications.
The evaluation criteria for the abbreviated applications are that the proposed pilot provide a federated, verified identity solution that meets the following requirements:

(1) Includes an effective identity proofing process (0 to 30 points). Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's approach to identity proofing.

(2) Enables multi-factor authentication (0 to 30 points). Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's approach to enabling multifactor authentication.

(3) Aligns with the Identity Ecosystem Framework Requirements (0 to 35 points). Reviewers will evaluate how well the applicant's proposed solution aligns with the IDEF requirements.

(4) Allow for interoperability with other federations in use in the public and private sectors (0 to 5 points). Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's approach to ensuring interoperability with other federated digital identity approaches.

2. Evaluation Criteria for Full Applications. The evaluation criteria that will be used in evaluating Full Applications are as follows:

a. Quality of the Planned Technical Solution (0 - 60 points)

(1) Privacy-Enhancing Capabilities (0 - 15 points): Reviewers will evaluate how well the applicant's proposed solution exhibits privacy-enhancing capabilities including:

- The manner in which it enables individuals and other pilot participants to have reliable assumptions about the personal information being processed by project participants (the project lead, contractors, subawardees and other collaborators);[9]
- The manageability of personal information, including the capability for alteration, deletion and selective disclosure. Such capabilities may include the mechanisms or design choices used to enable individuals to have control over or manage their personal information;[10]

[9] Processing means all actions of the system(s) that operate on personal information, including collection, generation or transformation, use, retention, disclosure or transmission and disposal.
[10] Although manageability capabilities may include mechanisms for individuals to have control over or manage their personal information, they may not be appropriate for all solutions. However, if the solution employs user consent or other user management controls, organizations should not use these controls to mitigate privacy risks created by architecture design or to mitigate risks that individuals cannot reasonably assess.

- The manner in which personal information or events can be processed without association or the potential for association with individuals beyond operational requirements;[11] and
- The controls implemented to mitigate privacy and civil liberties risks, including whether policy or technical measures are used for each risk, and why any, in any given case, (i) a policy measure is more appropriate than a technical measure and (ii) the project participant implementing the control is more appropriate than another project participant;

(2) Strength of Identity Proofing Approach (0 to 15 points): Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's proposed approach to leverage a secure and reliable method of identity proofing.

(3) Strength of Authentication Approach (0 to 10 points): Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's proposed approach to leverage a secure and reliable method of authentication.

(4) Supports Standards for Interoperability (0 to 5 points): Reviewers will evaluate how well the proposed solution complies with or leverages widely adopted interoperability standards and specifications, as appropriate, such as:

- Fast Identity Online (FIDO) (https://fidoalliance.org/specifications/overview/)
- Security Assertion Markup Language (SAML) (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)
- OpenID Connect (http://openid.net/foundation/)
- Open Authentication Standard (OAuth) (http://oauth.net/2/)
- User-Managed Access (UMA) (https://docs.kantarainitiative.org/uma/rec-uma-core.html)

(5) Usability across Total Population (0 to 10 points): Reviewers will evaluate how well the proposed solution enables disadvantaged or marginalized groups to obtain and use secure online credentials.

[11] Operational requirements on the solution should reflect the impossibility of completing the transaction without associating information to individuals. For example, identity proofing or providing direct health care services require association of information with an individual. Operational requirements cannot include the mere difficulty of disassociating the information from individuals or a project participant taking on a task that should be done by another participant. For example, system intermediaries' visibility into attribute values during transmission due to the difficulty of implementing encryption is not an acceptable operational requirement.

b. Quality of Implementation Plan (0 – 20 points).

Reviewers will evaluate the appropriateness, quality, completeness and effectiveness of the applicant's plans for implementation including providing an appropriate level of detail on the following: major task descriptions, schedule, quantified objectives, milestones, and measurable metrics that will be used to evaluate project success, method of evaluating the metrics, risks, and plans for stakeholder outreach and integration with other efforts to ensure solution meets market demands.

Specifically, reviewers will evaluate the following:

- The completeness of all participants' plans including any required contracting timelines, budget authorizations, and waiver requirements needed;
- How realistic and achievable are the measurable milestones set by the applicant, including metrics encompassing all work on the project including the state programs effected;
- The quality of the project leadership's plans to manage the project including managing the work of all project participants including sub-recipients, contractor's, etc., to ensure realization of project goals and objectives; and
- Alignment of the project plan to producing results consistent with the NSTIC Guiding Principles and IDEF requirements.

c. Impact Measures (0 - 10 points).

Reviewers will evaluate:

- The uniqueness of the contribution to the Identity Ecosystem**;**
- The number of potential users in the pilot and the number of potential users if the solution is fully deployed;
- The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into routine use expanding beyond initial pilot users and the award period;
- The potential for impacting the provision of state and local services within the state(s) involved in the pilot;
- The potential for impacting the provision of services states other than the pilot location(s); and
- The quality of described metrics.

d. Resource Availability (0 - 10 points).

Reviewers will evaluate:

- The appropriateness of the qualifications of the key personnel;
- The sufficiency of the time commitments of the key personnel;

- The appropriateness of the overall project resources to the project's scope and specific activities; and
- The cost-effectiveness of the project.

3. Selection Factors. The Selecting Official, who is the program manager of the NSTIC NPO, shall select applications for award based upon the rank order of the application. The Selecting Official may select an application out of rank based on one or more of the following selection factors:

a. The availability of Federal funds;
b. Whether the project duplicates other projects funded by NIST, DoC, or by other Federal agencies;
c. Diversity among the funded projects in state, local and tribal government programs addressed;
d. Geographic diversity among the pilots; and
e. Diversity of technical approaches across all funded projects to providing a foundation for the Identity Ecosystem.

The Selecting Official shall select Abbreviated Applications as finalists and Full Applications for recommendation for award based upon the application ranking and the selection factors above.

4. Review and Selection Process

a. Initial Administrative Review of Abbreviated and Full Applications. An initial review of timely received Abbreviated and Full applications will be conducted to determine eligibility, completeness, and responsiveness to this FFO. Responsiveness to the FFO includes identification of the government service(s) involved in the pilot project. Applications determined to be ineligible, incomplete, and/or non-responsive 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 which may easily be rectified or cured at a later point in the evaluation process.

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

(1) Abbreviated Applications. Each Abbreviated Application will be reviewed by at least three independent, objective reviewers, who are Federal employees, knowledgeable in the subject matter of this FFO and its objectives, and who are able to conduct a review based on the evaluation criteria for abbreviated applications (*see* Section V.1. of this FFO). While every application will have at least three reviews, applications may have differing numbers of reviews if specialized expertise is needed to evaluate the application. Based on the

reviewers' scores, a rank order will be prepared and provided to the Selecting Official for further consideration.

The Selecting Official will then select finalists based upon the rank order and the selection factors (*see* Section V.3. of this FFO). Applicants who submitted Abbreviated Applications that are chosen as finalists will have the opportunity to submit Full Applications.

(2) Full Applications. Each Full Application submitted by an applicant whose Abbreviated Application was selected as a finalist will proceed for review in accordance with the review and selection process below:

(a) Evaluation and Review. At least three independent, objective reviewers, who are Federal employees, knowledgeable in the subject matter of this FFO and its objectives will evaluate each application based on the evaluation criteria for full applications (*see* Section V.2. of this FFO). While every application will have at least three reviews, applications may have differing numbers of reviews if specialized expertise is needed to evaluate the application. These reviews will be forwarded to an Evaluation Board, a committee comprised of Federal employees knowledgeable in the subject matter of this FFO and its objectives.

The Evaluation Board will consider the reviewers' written evaluations based on the evaluation criteria (*see* Section V.2. of this FFO) and rank the applications through the use of numeric scores. Board members will then set a numeric score threshold for competitive applications based on the availability of funds.

Applicants whose applications were deemed competitive (i.e., applications above the threshold) may receive written follow-up questions in order for the Evaluation Board to gain a better understanding of the applicant's proposal. If deemed necessary, each competitive applicant will be invited to participate in a web conference, or an in-person meeting with the Evaluation Board. Applicants may also be asked to provide updated commitment letters from potential project participants at that time. As a result of the additional information, the Evaluation Board members may revise their assigned numeric scores.

(b) Ranking and Selection. Based on the Evaluation Board members' final numeric scores, a final rank order will be prepared and provided to the Selecting Official for further consideration. The Selecting Official will then recommend applications for funding based upon the rank order and the selection factors (*see* Section V.2. of this FFO).

NIST reserves the right to negotiate the budget costs with the selected applicant. Negotiations may include requesting that the applicant remove certain costs.

Additionally, NIST may request that the applicant 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. The final approval of selected applications and issuance of awards will be by the NIST Grants Officer. The award decisions of the Grants Officer are final.

c. 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.

5. Anticipated Announcement and Award Date. Review of Full Applications, selection of successful applicants, and award processing is expected to be completed in August 2016. The earliest anticipated start date for awards under this FFO is expected to be September 1, 2016.

6. Additional Information

a. Notification to Unsuccessful Applicants. Unsuccessful applicants will be notified in writing.

b. Notification to Applicants of Finalist Applications. NIST will send written invitations to submit Full Applications to applicants whose Abbreviated Applications were selected as finalists.

c. **Retention of Unsuccessful Applications.** An electronic copy of each non-selected Abbreviated and Full Application will be retained for three years for record keeping purposes. After three years, it will be destroyed.

d. **Protection of Proprietary Information.** When an application includes trade secrets or information that is commercial or financial, or information that is confidential or privileged, it is furnished to the Government in confidence with the understanding that the information shall be used or disclosed only for evaluation of the application. Such information will be withheld from public disclosure to the extent permitted by law, including the Freedom of Information Act. Appropriate labeling in the application aids NIST in the identification of what information may be specifically exempt from disclosure. Without assuming any liability for inadvertent disclosure, NIST will seek to limit disclosure of such information to its employees and to outside reviewers when necessary for merit review of the application or as otherwise authorized by law. This restriction does not limit the Government's right to use the information if it is obtained from another source.

e. **Changes in Applicant and/or Requested Funding Amount.** An applicant with a successful Abbreviated Application may change the lead entity prior to submission of the Full Application. Both the original applicant and new entity must provide written notice to Barbara Cuthill by e-mail to nstic@nist.gov in order to do so. The new entity must also be an eligible applicant. Any applicant may also revise the requested budget amount for the Full Application.

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 http://go.usa.gov/SNMR.

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 FFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if you seek the information at this link and it is no longer working or you need more information.

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 FFO, Federal Awarding Agency Contacts, Grant Rules and Regulations, if you seek the information at this link and it is no longer working or you need more information.

d. **Funding Availability and Limitation of Liability.** Funding for the program listed in this notice is contingent upon the availability of Fiscal Year 2016 appropriations. NIST issues this notice subject to the appropriations made available under the current continuing resolution funding the Department of Commerce, the Continuing Appropriations Act, 2016 (as amended, December 16, 2015). NIST anticipates making awards for the program listed in this notice provided that funding for the program is continued beyond December 22, 2015, 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.** All applications should include a description of any work proposed to be performed by an entity other than the applicant, and the cost of such work should ordinarily be included in the budget.

   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. Questions about these requirements may be directed to Chief Counsel for NIST, (301) 975-2803, nistcounsel@nist.gov.

Any use of NIST-owned intellectual property by an applicant 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.

If any inventions made in whole or in part by a NIST employee arise in the course of an award made pursuant to this FFO, the United States government may retain its ownership rights in any such invention. Licensing or other disposition of NIST's rights in such inventions will be determined solely by NIST, and include the possibility of NIST putting the intellectual property into the public domain.

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, 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 activity.

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 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.** NIST reserves the right to make an independent determination of whether an applicant's activities include research involving human subjects. NIST will conduct an independent administrative review of all applications accepted for funding that include research involving human subjects that were approved by a non-NIST Institutional Review Board (IRB). Research may not start until the NIST Human Subjects Protection Office (HSPO) issues institutional review approval for final action by the NIST Grants Officer. (15 C.F.R. § 27.112 Review by Institution.) If NIST determines that an application includes research activities which involve human subjects, the applicant will be required to provide additional information for review and approval. The documents required for funded proposals are listed in each

section below. Most such 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. If an award is issued, no research activities involving human subjects shall be initiated or costs incurred for those activities under the award until the NIST Grants Officer issues written approval. Retroactive approvals are not permitted.

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:

   (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. 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 will be provided.
(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.

c. 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).

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 NSTIC NPO 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 contain information as prescribed in 2 C.F.R. § 200.328 and include key metrics indicating project status such as number of actual users, number of transactions, etc.

(3) Participate in and report to the IDESG. Each award recipient is expected to report twice a year at meetings of the IDESG on pilot progress, accomplishments, challenges and lessons learned. Only non-proprietary, publicly releasable information will be provided at these presentations. In addition, each award recipient will be required to actively participate on at least two committees of the IDESG and provide contributions stemming from lessons learned in the pilot.

(4) NSTIC NPO Program Management. Each award recipient is expected to participate in a kickoff meeting within the first thirty days of award and detailed design reviews within sixty days of award. These design reviews will include the details of the technical design of the solution overview such as architecture, data flows (including flows of personal information), interfaces, use cases risks and plans for mitigating those risks, etc., as well as demonstrate how the pilot meets the NSTIC Guiding Principles. In addition, the NSTIC NPO can require additional specialized reviews against any of the NSTIC Guiding Principles or specific aspects of the solution, as needed.

(5) Program Evaluation. NIST will be arranging for an outside organization to evaluate the success of pilot projects awarded under this cooperative agreement program. Recipients receiving a cooperative agreement under this program will be required to cooperate with the organization performing the evaluation. This may involve sharing proprietary or confidential information with the evaluator as well as the NSTIC National Program Office. Proprietary or confidential information will not be included in any published reports.

(6) Program Communication. All pilot projects awarded under this program are expected to publish interim reports on the publicly releasable lessons learned from their projects to benefit similar state and local government efforts**.**

(7) Patent and Property Reports. From time to time, and in accordance with the Uniform Administrative Requirements (*see* Section VI.2. of this FFO) and other

terms and conditions governing the award, the recipient may need to submit property and patent reports.

(8) 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 FFO, 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.

VII. Federal Awarding Agency Contacts

Questions should be directed to the following contact persons:

Subject Area	Point of Contact
Programmatic and Technical Questions	Barbara Cuthill Phone: 301-975-3273 E-mail: nstic@nist.gov
Technical Assistance with Grants.gov Submissions	Christopher Hunton Phone: 301-975-5718 Fax: (301) 975-8884

	E-mail: grants@nist.gov Or Grants.gov Phone: (800) 518-4726 E-mail: support@grants.gov
Grant Rules and Regulations	Dean Iwasaki Phone: 301-975-8449 Fax: (301) 975-8884 E-mail: dean.iwasaki@nist.gov

VIII. Other Information

Webinar (Applicants' Conference): NIST will hold a webinar (Applicants' Conference) to provide general information regarding NSTIC, to offer general guidance on preparing applications, and to answer questions. Proprietary technical discussions about specific project ideas with NIST staff are not permitted at this conference or at any time before submitting the application to NIST. Therefore, applicants should not expect to have proprietary issues addressed at the Applicants' Conference. Also, NIST/NSTIC Program staff will not critique or provide feedback on project ideas while they are being developed by an applicant. However, NIST/NSTIC Program staff will answer questions about the NSTIC Program eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application at the Applicants' Conference and by phone and email. Attendance at the Applicants' Conference is not required. Information on the Applicants' Conference is available at http://www.nist.gov/nstic/funding-opportunities.html.