January 16, 2014

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

- **Announcement Type:** Initial

- **Funding Opportunity Number:** 2014-NIST-NSTIC-01

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

- **Dates:** Abbreviated Applications must be received electronically through Grants.gov no later than 11:59 p.m. Eastern Time, Thursday, March 6, 2014. Abbreviated Applications received after this deadline will not be reviewed or considered. Review of Abbreviated Applications and selection of finalists is expected to be completed by Tuesday, April 1, 2014. The selected finalists will then be invited to submit a Full Application including a Technical Proposal shortly following their selection as a finalist. Full Applications must be received electronically through Grants.gov no later than 11:59 p.m. Eastern Time, Tuesday, May 13, 2014. Full Applications received after this deadline will not be reviewed or considered. Review of Full Applications, selection of successful applicants, and award processing is expected to be completed in August 2014. The earliest anticipated start date for awards under this FFO is expected to be September 1, 2014.

  If you are invited to submit a Full Application, keep in mind when developing your submission timeline that (1) a free annual registration process in the electronic System for Award Management (SAM) (*see* Section VI.2.b. of this FFO) may take more than two weeks, and (2) applicants using Grants.gov will receive a series of receipts over a period of up to two business days before learning via a validation or rejection notification whether a Federal agency's electronic system has received its application.

- **Application Submission Address:** See Section IV. in the Full Announcement Text of this FFO**.**

- **Funding Opportunity Description:** NIST is soliciting applications from eligible applicants to pilot online identity solutions that embrace and advance the NSTIC vision: that individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice, and innovation. Specifically, the Federal government seeks to initiate and support pilots that address the needs of individuals, private sector organizations, and all levels of government in accordance with the NSTIC Guiding Principles that identity solutions will be (1) privacy-enhancing and voluntary, (2) secure and resilient, (3) interoperable, and (4) cost-effective and easy-to-use. NIST will fund projects that are intended to test or demonstrate new solutions, models, and frameworks that either do not exist or are not widely adopted in the marketplace today.

- **Anticipated Amounts:** NIST anticipates that awards will be in the range of approximately $1,250,000 to $2,000,000 per year per project for up to two (2) 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 with lower funding amounts. The number of projects funded will depend on the amount of available funds. Fiscal Year (FY) 2014 appropriations for the NSTIC NPO have not been determined at the time of publication, but the maximum possible amount for new awards is not expected to exceed $6 million.

- **Funding Instrument:** Cooperative agreement.

- **Who Is Eligible:** Accredited institutions of higher education; hospitals; non-profit organizations; commercial organizations; and state, local, and Indian tribal governments located in the United States and its territories. An eligible organization may work individually or include proposed subawardees, contractors or other collaborators in a project, effectively forming a team or consortium. An organization may submit more than one application but each must be on a distinct topic. 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 public meeting (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 www.nist.gov/nstic.**

FULL ANNOUNCEMENT TEXT

I. Funding Opportunity Description

The statutory authority for the National Strategy for Trusted Identities in Cyberspace (NSTIC) 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's vision is: Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

NSTIC acknowledges and addresses three major challenges in cyberspace:

1. A lack of confidence and assurance that people, organizations, and businesses are who they say they are online and that devices are trusted and authentic. Both businesses and governments are unable to offer many services online because they cannot effectively identify the individuals with whom they interact.

2. The current online environment presents a de facto requirement that individuals maintain dozens of different usernames and passwords, typically one for each Web site with which they interact. The complexity of this approach is a burden to individuals, and it encourages behavior – like the

reuse of passwords – that makes online fraud and identity theft easier. At the same time, online businesses face ever-increasing costs for securely managing customer accounts, consequences of online fraud, and the loss of business that results from individuals' unwillingness to create yet another account. Spoofed Web sites, stolen passwords, and compromised accounts are all symptoms of inadequate authentication mechanisms.

3. There is a growing list of online privacy challenges, ranging from minor nuisances and unfair surprises to injury or discrimination based on sensitive personal attributes that are improperly disclosed, actions and decisions in response to misleading or inaccurate information, and costly and potentially life-disrupting identity theft. In the aggregate, even the harms at the less severe end of this spectrum have significant adverse effects, because they continue to undermine consumer trust in the Internet environment. Diminished trust causes consumers to hesitate before adopting new services and impedes innovative and productive uses of new technologies.

NSTIC envisions addressing these challenges through a user-centric **Identity Ecosystem,** defined in the Strategy 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."[1]

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 Identity Ecosystem is designed to securely support transactions that range from anonymous to fully-authenticated and from low- to high-value. The Identity Ecosystem, as envisioned by NSTIC, will increase:

- **Privacy protections** for individuals, who will be able to trust that their personal data is handled fairly and transparently;
- **Convenience** for individuals, who may choose to manage fewer passwords or accounts than they do today;
- **Efficiency** for organizations, which will benefit from a reduction in paper-based and account management processes;
- **Ease-of-use**, by automating identity solutions whenever possible and basing them on technology that is simple to operate;
- **Security**, by making it more difficult for criminals to compromise online transactions;
- **Confidence** that digital identities are adequately protected, thereby promoting the use of online services;
- **Innovation**, by lowering the risk associated with sensitive services and by enabling service providers to develop or expand their online presence; and
- **Choice**, as service providers offer individuals different—yet interoperable—identity credentials and media.

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

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

In 2012, NIST funded the creation of the Identity Ecosystem Steering Group (IDESG), a private sector-led organization charged with crafting an Identity Ecosystem Framework which continues to foster the emergence of the identity ecosystem. NIST also funded five (5) pilot projects in the initial round of the NSTIC pilot cooperative agreements. In 2013, NIST funded an additional five (5) pilot projects, two (2) projects piloting technology for accessing state government services, and one (1) third-party evaluation of the state government services projects. Descriptions of the pilot projects are available on the NSTIC website at http://www.nist.gov/nstic/pilot-projects.html.

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 easy to use trusted digital identity credentials that will improve trust in online transactions while enabling the market in online credentials to flourish.

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

Pilots Program Focus Area: Building Identity Ecosystem Foundations and Frameworks to Address Barriers

The purpose of the NSTIC Pilots Cooperative Agreement Program is to advance the NSTIC vision, objectives and guiding principles, and tackle barriers that have, to date, impeded the Identity Ecosystem from being fully realized. NIST will fund pilot projects that will make something happen that otherwise would not (i.e., the pilot projects will test or demonstrate new solutions, models and frameworks that either do not exist or are not widely adopted in the marketplace today). The NSTIC NPO defines pilots as systems deployed in production environments which include a limited number of 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 identity solutions marketplace has struggled, in part, due to a number of barriers that market forces alone have been unable to overcome. These barriers include, but are not limited to:

- A dearth of identity solutions and trust frameworks—or those with limited capabilities–that cross multiple sectors, making it difficult for the benefits of successful identity solutions in one sector to be realized across others.
- A lack of common standards for security, privacy, performance benchmarking, and data use.
- The dissonance arising from rapidly changing technology and its impact on individual privacy and civil liberties.
- Lack of clarity on liability and other complex economic issues (e.g., "who is liable if something goes wrong in a transaction?" "How – if at all – should transactions be monetized?").
- A lack of commonly accepted technical standards to ensure interoperability among different authentication solutions.
- Challenges with usability of some strong authentication technologies.
- Challenges with balancing transparency to individual users and ease-of-use.

Specifically, the NSTIC NPO is interested in funding projects with innovative approaches that address some or all of these barriers in a way that aligns with and advances the NSTIC's four guiding principles. These projects can thus provide a foundation upon which the Identity Ecosystem can be constructed.

Examples of objectives that projects may strive to achieve include, but are not limited to:

1. Demonstrate the feasibility of the Identity Ecosystem and reusable credentials via projects that interoperably and securely link multiple sectors via trust frameworks, including multiple identity providers (IDPs) and relying parties.
2. Expand the acceptance and use of trust frameworks and third-party credential providers by RPs.
3. Create and demonstrate solutions that can help public and private sector entities alike more easily jumpstart adoption of trusted strong authentication technologies in lieu of passwords at public-facing websites, for example, pilots have included secure and reliable identity exchange hubs that can quickly validate and process strong credentials across multiple trust frameworks, while enabling enhanced privacy and civil liberties protections.
4. Create user-centric solutions to address the limitations and barriers that have inhibited consumer demand for strong authentication technologies and incentivize consumers to obtain a strong credential. For example, demonstrate how advances in usability and accessibility can improve user comfort with and uptake of strong authentication technologies.
5. Create and demonstrate a framework of policies, rules of behavior, and agreements among Identity Ecosystem stakeholders that can be applied across multiple trust frameworks and provides:
    a. increased certainty on liability and other economic issues;
    b. a strong set of privacy and civil liberties protections for all Identity Ecosystem participants, focused on fully addressing the issues outlined in Objective 1.1 of NSTIC, "Establish improved privacy protection mechanisms" (*see* p. 29-30 of the Strategy identified in Section I. of this FFO); and
    c. a means for establishing and implementing quantifiable and reproducible levels of assurance for credentials.
6. Demonstrate privacy-enhancing technologies that mitigate privacy and civil liberties risks, such as increased tracking and personal data aggregation in today's online environment, and can also support viable business models, current security requirements, and generally accepted performance standards.
7. Demonstrate interoperability across multiple solutions types (e.g., smart cards, one time passwords, other technologies) in an identity ecosystem.
8. Create and demonstrate frameworks, methodologies, or solutions for enabling the exchange of specific attributes associated with identities while minimizing the sharing of non-essential information.
9. Demonstrate innovative approaches to usability and providing end-user transparency.
10. Demonstrate the role that public sector entities can play in helping individuals prove their identity to private sector credential providers and/or RPs.

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 NSTIC. In addition, project participants must possess a demonstrated record of excellence in identity management efforts.

II. Award Information

1. Funding Instrument. The funding instrument that will be used is a cooperative agreement. The nature of NIST's "substantial involvement" will generally be collaboration between NIST and the recipient organizations. This includes NIST collaboration with a recipient on the scope of work. Additional forms of substantial involvement that may arise are described in Chapter 5.C of the Department of Commerce (DoC) Grants and Cooperative Agreements Manual, which is available at http://www.osec.doc.gov/oam/grants_management/policy/documents/FINAL%20Master%20DOC%20Grants%20Manual%202013%20(03.01.13)_b.pdf.

2. **Multi-Year Funding Policy.** When an application for a multi-year award is approved, funding will usually be provided for only the first year of the project. If a project is selected for funding, NIST has no obligation to provide any additional funding in connection with that award. Continuation of an award to increase funding or extend the period of performance is at the sole discretion of NIST. Continued funding will be contingent upon satisfactory performance, continued relevance to the mission and priorities of NSTIC, and the availability of funds.

3. **Funding Availability.** NIST anticipates that awards will be in the range of approximately $1,250,000 to $2,000,000 per year per project for up to two (2) 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 with lower funding amounts. The number of projects funded will depend on the amount of available funds. FY 2014 appropriations for the NSTIC NPO have not been determined at the time of publication, but the maximum possible amount for new awards is not expected to exceed $6 million.

III. Eligibility Information

1. **Eligible Applicants.** Eligible applicants are accredited institutions of higher education; hospitals; non-profit organizations; commercial organizations; and state, local, and Indian tribal governments located in the United States and its territories. An eligible organization may work individually or include proposed subawardees, contractors or other collaborators in a project, effectively forming a team or consortium. An organization may submit more than one application but each must be on a distinct topic. Federal agencies may participate in projects but may not receive NIST funding.

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

3. **Other**

   Abbreviated Applications. NIST requires Abbreviated Applications under the NSTIC Pilots Cooperative Agreement Program. Only applicants whose Abbreviated Applications have been selected as finalists will be invited to submit Full Applications.

IV. Application Submission Information

1. **Address to Request Application Package.** The application form for the Abbreviated Application, the SF-424, is available at www.grants.gov. The SF-424 may also be requested by contacting the NIST personnel listed below.

   Dr. Barbara Cuthill, National Institute of Standards and Technology, NSTIC Pilots Cooperative Agreement Program, 100 Bureau Drive, Mail Stop 2000, Gaithersburg, MD 20899-2000. Phone: 301-975-3273, e-mail barbara.cuthill@nist.gov.

2. **Application Content and Format**

a. **Required Abbreviated Application Form and Documents**

   The Abbreviated Applications must be received electronically through 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. The FFO number 2014-NIST-NSTIC-01 must be identified in item 12 of the SF-424. The list of certifications and assurances referenced in item 21 of the SF-424 is not needed for the Abbreviated Application.

(2) Abbreviated Proposal. A word-processed document written by the applicant of no more than four (4) pages describing the proposed project that includes sufficient information to address the evaluation criteria (*see* Section V.1. of this FFO). **The Abbreviated Proposal should be 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.**

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 for their "finalist" application are permitted to submit Full Applications to NIST for the NSTIC Pilots Cooperative Agreement Program. Full Applications submitted by applicants who have not been selected as finalists, and Full Applications submitted by applicants who did not submit an Abbreviated Application, will be returned to the applicant without review. 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. The FFO number 2014-NIST-NSTIC-01 must be identified in item 12 of the SF-424. The list of certifications and assurances referenced in item 21 of the SF-424 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 two (2) 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 word-processed 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 detailing the challenge (or challenges) the pilot will address, as well as clear, measurable performance objectives that can be used to determine the potential success of the proposed pilot project. The Technical Proposal should contain the following information:

(a) Executive Summary. An executive summary of the proposed approach including references to the challenge(s) or barrier(s) to the Identity Ecosystem addressed in the proposal and the use cases to be piloted. 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 barrier(s) or challenge(s) to the Identity Ecosystem and how the specific objectives of the project will address the barrier(s) or challenge(s). Be clear about what this project would fund that otherwise would not happen. The NSTIC NPO has identified the barriers and challenges listed in Section I. of this FFO. If the proposed project addresses barrier(s) or challenge(s) not listed in Section I. of this FFO, the applicant must provide a justification for why the barrier(s) or challenge(s) is (are) impeding the emergence of the Identity Ecosystem. This section should also provide information on the use cases that the pilot addresses and why the applicant chose those use cases. This section establishes that the proposed project is within the scope of the FFO and provides critical background for the discussion of the proposed operational pilot.

(c) Operational pilot. A description of 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 solutions discussed in the pilot project, how they interconnect, and what key information is exchanged among the components. An architecture diagram and data flow diagram 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. A mapping to the derived NSTIC requirements may help describe how the pilot implements the NSTIC Guiding Principles. (For more on the NSTIC derived requirements see http://nstic.blogs.govdelivery.com/2013/09/11/what-does-it-mean-to-embrace-the-nstic-guiding-principles/.) This section should also provide an estimate of the planned number of end users and the minimum number of end users needed to be successful, including both credentials issued and relying parties, in each phase of the pilot.

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, policy should not be used to mitigate a technical architecture that by its design creates privacy or civil liberties risks. This section should explain how the technical and/or policy measures are used to address all eight Fair Information Privacy Principles listed in Appendix A of the Strategy identified in Section I. of this FFO.

This section should address the *Adherence to the NSTIC Guiding Principles* evaluation criterion (*see* Section V.1.a. of this FFO).

(d) Statement of Work and Implementation Plan. A statement of work that discusses the specific proposed tasks, including a schedule of measurable events and milestones as well as clear, measurable performance objectives that can be used to determine the success of the pilot project. The statement of work must include all project participants including any relying parties and any planned efforts to disseminate information and reach out to users. 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, Work Breakdown Structure 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 large scale use, and a description of any planned role(s) of the project participants in the Identity Ecosystem Steering Group. 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 and proposed roles of the project participants, including the proposed role of the project lead and of each subwardee, contractor or other collaborator in the project. In addition, this section should include a description of the qualifications, including skills and experience and role of all key personnel on the project. The key personnel should include at least one individual from each participant, with time commitments provided. The key personnel should include at least one privacy expert familiar with both policy and technical aspects of privacy needs committed to working with the project. Also, at least one usability expert and a project manager are needed.

This section and the budget narrative 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. Only allowable costs should be included in the budget. Information on cost allowability is available in the Supplemental Information, section B.1 of the DoC Pre-Award Notification Requirements for Grants and Cooperative Agreements, which are contained in the Federal Register notice of December 17, 2012 (77 FR 74634), and are available at https://www.federalregister.gov/articles/2012/12/17/2012-30228/department-of-commerce-pre-award-notification-requirements-for-grants-and-cooperative-agreements. Information needed for each category is as follows:

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

(b) Fringe Benefits – Fringe benefits should be identified separately from salaries and wages and based on rates determined by organizational policy. The items included in the fringe benefit rate (health insurance, parking) 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.) that is 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 to these meetings 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.

For awards to commercial organizations, audits may be required by an external auditor (CPA or cognizant Federal agency), as specified in the award. If a recipient has never received Federal funding from any Federal agency, a certification may be required from a CPA to determine whether the recipient has a functioning financial management system that meets the provisions of 15 C.F.R. § 14.21. Therefore, costs for these audits and certification should be included in the budget accordingly.

(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 agency. If the rate was not established by a cognizant Federal agency, provide a statement to this effect. Successful applicants will be required to obtain such a rate.

(9) Letters of Commitment or Interest. Letters are not included in the page count.

(a) Letters of Commitment to participate, as applicable. If the application identifies third parties including contractors, subawardees, and/or other collaborators who will participate in the proposed project, effectively forming a team or consortium, 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 and what they will be doing for the project. A letter is required whether or not the organization is receiving Federal funds.

(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.

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.(9) 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 indicating an application is received does not provide information about whether attachments have been received.***

c. Application Format

(1) 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) Line Spacing. Applicants can use single spacing or double spacing.

(5) Margins. One (1) inch top, bottom, left, and right.

(6) Page layout. Portrait orientation only except for figures, graphs, images, and pictures.

(7) 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.

(b) For Full Applications:

Page limit includes: Table of contents (if included), Technical Proposal with all required sections, 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 or Work Breakdown Structure or other planning document (if included); Architecture and data flow diagrams (if included); Privacy Impact Assessment (PIA) and/or Privacy Evaluation Matrix (PEM)(if included); Budget Narrative; and Indirect Cost Rate Agreement, letters of interest, letters of commitment.

(8) Page numbering. Number pages sequentially.

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

(10) Application language. English.

3. Submission Dates and Times. Abbreviated Applications must be received electronically through Grants.gov no later than 11:59 p.m. Eastern Time, Thursday, March 6, 2014. Abbreviated Applications received after this deadline will not be reviewed or considered. Review of Abbreviated Applications and selection of finalists is expected to be completed by Tuesday, April 1, 2014. The selected finalists will then be invited to submit a Full Application including a Technical Proposal shortly following their selection as a finalist. Full Applications must be received electronically through Grants.gov no later than 11:59 p.m. Eastern Time, Tuesday, May 13, 2014. Full Applications received after this deadline will not be reviewed or considered. NIST will consider the date and time stamped on the validation generated by www.grants.gov as the official submission time.

NIST strongly recommends that applicants do not wait until the last minute to submit an application. NIST will not make allowance for any late submissions. To avoid any potential processing backlogs due to last minute Grants.gov registrations, applicants are highly encouraged to begin their Grants.gov registration process well ahead of the submission deadline.

When developing your submission timeline, keep in mind that (1) a free annual registration process in the electronic System for Award Management (SAM) (*see* Section VI.2.b. of this FFO) may take more than two weeks, and (2) applicants using Grants.gov will receive a series of receipts over a period of up to two business days before learning via a validation or rejection notification whether a Federal agency's electronic system has received its application.

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

5. Funding Restrictions. Profit or fee is not an allowable cost.

6. Other Submission Requirements

a. Applications must be submitted electronically. Electronic applications must be submitted via Grants.gov at www.grants.gov, under announcement 2014-NIST-NSTIC-01.

(1) Submitters of electronic applications should carefully follow specific Grants.gov instructions to ensure the 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 2014-NIST-NSTIC-01 announcement, contact Christopher Hunton by phone at 301-975-5718 or by e-mail at christopher.hunton@nist.gov.

(2) 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 Dun and Bradstreet Data Universal Numbering System (DUNS) number (*see* Section VI.2.b) 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. 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 authorized individual(s) 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.

(3) 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 the "Grant Applicants" page.

In addition to following the "Steps" and instructions described in the "Applicant Actions" section and its sub-categories, further detailed instructions are described in "Applicant Resources" and all of its subcategories. This appears in the box near the top left of the Grant Applicants page. Applicants should follow the links associated with each subcategory.

Applicants will receive a series of receipts during a process of up to two business days before the application is either validated as electronically received by the Federal agency system, or rejected by it. 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 instructions 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.

Refer to important information in Section IV.3. 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 for grants.gov FFO amendments or may request copies from Dr. Barbara Cuthill by telephone at (301) 975-3273 or by e-mail to barbara.cuthill@nist.gov.

V. Application Review Information

1. Evaluation Criteria. The evaluation criteria that will be used in evaluating Abbreviated and Full Applications are as follows:

a. Adherence to NSTIC Guiding Principles (0 - 40 points, sub-criteria a. through d. below receive equal weight). Explain how the operational pilot meets the following guiding principles as supported by the description of the operational pilot, including its architecture and data flows. Mapping critical elements to the NSTIC derived requirements is also helpful. (For more on the NSTIC derived requirements see http://nstic.blogs.govdelivery.com/2013/09/11/what-does-it-mean-to-embrace-the-nstic-guiding-principles/.) Compliance with the Guiding Principles requires specific supporting discussion of what will be done in the project.

i. Privacy-enhancing and voluntary – The envisioned Identity Ecosystem will mitigate privacy and civil liberties risks engendered by today's online environment of identification, tracking, and personal data aggregation. Such mitigation will be grounded in conformance to the Fair Information Practice Principles (FIPPs) (*see* Appendix A of the Strategy[2]) in order to provide multi-faceted privacy protections.

Reviewers will be looking for specific details on how privacy and civil liberties will be protected and how that protection will be implemented on both a technical and policy level. Implementation details can be provided in a Privacy Impact Assessment (PIA), Privacy Evaluation Matrix (PEM) and/or mapping of the pilot details to FIPPs. In particular, reviewers will be looking for a demonstrated understanding of the privacy or civil liberties risks raised by the application and the appropriateness of mitigations for such risks, including:

(1) How the application:

- Addresses any collection, use, and disclosure or transmission of personal information;
- Addresses when and in what manner users will be provided with information about how project participants (the project lead, contractors, subawardees and other collaborators) collect, use, disseminate, and maintain personal information, as well as how individuals can control their personal information and attributes;
- Addresses why and for how long personal information will be retained, the appropriateness of the development of any new databases of personal information, as well as security measures for any such retention;
- Minimizes retention of personal information;
- Minimizes data aggregation and linkages across transactions;
- Provides appropriate mechanisms to allow individuals to access, correct, and delete personal information;
- Establishes accuracy standards for personal information used in identity assurance, authentication or authorization solutions;
- Protects, transfers at the individual's request, and securely destroys personal information when terminating business operations or overall participation in the Identity Ecosystem;
- Accounts for how personal information is actually collected, used, disclosed or transmitted and retained, and provides mechanisms for compliance, audit, and verification; and
- Provides effective redress mechanisms for, and advocacy on behalf of, individuals who believe their personal information may have been misused.

(2) Identifying how FIPPs will be used to address the topics in section (i) above; whether they will be implemented by policy and/or technical measures, although policy measures should not be used to mitigate privacy or civil liberties risks created by the technical design of the project; which project participant(s) will be responsible for the implementation; and supporting performance metrics for such implementations; and

[2] Available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

(3) Describing what role, if any, trust frameworks will play in the enforcement of a common privacy framework applicable to all project participants, including IdPs, APs, brokers and RPs.

ii. **Secure and resilient** – Security ensures the confidentiality, integrity and availability of identity solutions, and the non-repudiation of transactions. Credentials are resilient when they can easily and in a timely manner recover from loss, compromise, or theft and can be effectively revoked or suspended in instances of misuse. In addition to credentials, information stores also need to be protected.

Reviewers will be looking for specific details on how solutions are secure and resilient. Examples of such details may include, but are not limited to:

- How new or existing Trust Frameworks ensure all project participants adhere to appropriate, risk-based levels of security.
- How solutions embrace security mechanisms that provide material security advances over the password-based regime dominant in the marketplace today.
- How solutions will provide secure and reliable methods of electronic authentication.
- How solutions demonstrate the integration of all major aspects of the project.

iii. **Interoperable** – Interoperability enables service providers to accept a variety of credentials and identity media and also supports identity portability enabling individuals to use a variety of credentials in asserting their digital identity to a service provider. Interoperability needs to go beyond standards conformity to address policy and procedural interoperability. Reviewers will be looking for applications that foster the reduction and elimination of policy and technology silos and adhere to open standards. Proprietary solutions that limit interoperability will be less competitive.

Reviewers will be looking for specific details on how proposed solutions are interoperable. Examples of such details may include, but are not limited to:

- How new or existing Trust Frameworks ensure all project participants adhere to common standards, policies, and rules and ensure proper and consistent treatment of personal data.
- How solutions leverage existing standards and/or demonstrate the need for new standards and an ability to materially advance the development and adoption of new standards.
- How solutions can be used across multiple sectors and RPs.
- How individual credentials are simply and securely portable between RPs with appropriate notifications to individuals.

iv. **Cost-effective and easy to use** – Identity solutions should be simple to understand, intuitive, easy-to-use, and enabled by technology that requires minimal user training. This can be achieved with the thoughtful integration of usability principles and user-centered design. Many existing technology components in widespread use today (e.g., mobile phones, smart cards, and personal computing devices) can be leveraged to act as or contain a credential.

Reviewers will be looking for specific details on how solutions are cost-effective and easy to use. Examples of such details may include, but are not limited to:

- How new or existing Trust Frameworks can lower costs for all Identity Ecosystem stakeholders and erase barriers to usability.
- How solutions do not present significant usability challenges.

- How solutions propose innovative applications of technology that enhance usability, relative to current market solutions.
- How costs per user are not prohibitive and can grow the Identity Ecosystem in accordance with NSTIC's four guiding principles (*see* Section I of this FFO).
- How solutions lower barriers for user acceptance and can be easily incorporated into current user activities.
- How service level agreements provide easy to understand opt-in choices for the consumer to use a service.

b. Quality of Implementation Plan (0 - 30 points). Quality of the applicant's plans for implementation including details on the following: tasks, schedule, quantified objectives, milestones, metrics, method of evaluating the metrics, risks, and plans for stakeholder outreach and integration with other efforts. The implementation plans should include all project participants including relying parties' activities during the project. Measurable milestones tied to metrics need to be established throughout the project for demonstrating progress in all areas relevant to the overall pilot. Milestones should be realistic and achievable in the allotted timeframes with the proposed resources. All aspects discussed as part of the solution should be included in the implementation plan and have associated milestones. Milestones should reflect the work of all participants on the project including relying parties.

c. Contribution to Identity Ecosystem (0 - 20 points). Explain how the operational pilot will contribute to the Identity Ecosystem in the following areas:

- **Unique Contribution** – The contribution that this project would make to the identity ecosystem that absent NSTIC project funding would not occur.
- **Large Scale Use** – The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into production expanding beyond initial pilot users.
- **Contribution to the Identity Ecosystem Steering Group (IDESG)** – How the applicant intends to interact and engage with the IDESG to support the development of the Identity Ecosystem Framework.

d. Resource Availability (0 - 10 points). Reviewers will be looking for details on:

- The qualifications and commitment of the identified project participants including key personnel, and previously demonstrated ability to achieve positive outcomes in pilot programs and similar endeavors. A subject matter expert with specialized knowledge of privacy technology and policy issues is expected on all projects. All participating organizations are expected to identify at least one key person and that person's time commitment.
- The appropriateness of proposed resources including personnel compared to the project's scope, as well as the cost-effectiveness of the project in using available resources to complete the project.

2. Selection Factors. The Selecting Official, who is the Senior Executive Advisor for Identity Management, shall select Abbreviated Applications as finalists to submit Full Applications. The Selecting Official will also select Full Applications for award based upon the application ranking. The Selection 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 successfully addressing a variety of barriers that have to date impeded the Identity Ecosystem from being fully realized.
d. Diversity of technical approaches across all funded projects to providing a foundation for the Identity Ecosystem.

e. Diversity in the gaps in the emerging Identity Ecosystem addressed by the funded projects.

3. 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 and the scope of the stated program objectives. Applications determined to be ineligible, incomplete, and/or non-responsive may be eliminated from further review.

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 (3) 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 (*see* Section V.1. of this FFO). 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 to submit Full Applications based upon the rank order and the selection factors (*see* Section V.2. of this FFO).

(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 (3) 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 (*see* Section V.1. of this FFO). These reviews will be forward 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.1.of this FFO) and rank the applications. Board members will then set a threshold for competitive applications based on the availability of funds.

Competitive applications (i.e., applications above that threshold) may receive written follow-up questions in order for the Evaluation Board to gain a better understanding of the applicant's proposal. Once the Evaluation Board has completed their review of the applicant's responses, a teleconference or web conference may be deemed necessary. If deemed necessary, each competitive applicant will be invited to participate in a teleconference or web conference 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 select funding recipients 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. For international

applications, NIST will follow applicable U.S. laws and policies. NIST may select part, some, all, or none of the applications. 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.

4. **Anticipated Announcement and Award Dates.** Review of Abbreviated Applications and selection of finalists is expected to be completed by Tuesday, April 1, 2014. Review of Full Applications, selection of successful applicants, and award processing is expected to be completed in August 2014. The earliest anticipated start date for awards made under this FFO is expected to be September 1, 2014.

5. **Additional Information**

a. **Application Replacement Pages.** Applicants may not submit replacement pages and/or missing documents once an application, abbreviated or full, has been submitted. Any revisions must be made by submission of a new, Abbreviated or Full Application, by the respective submission deadline via Grants.gov.

b. **Notification to Unsuccessful Applicants.** Unsuccessful applicants will be notified in writing.

c. **Notification to Finalists.** Applicants whose Abbreviated Applications are selected by NIST as "finalists" will be notified in writing and invited by NIST to submit Full Applications for the selected Abbreviated Applications.

d. **Retention of Unsuccessful Applications.** An electronic copy of each non-selected Abbreviated and Full Application will be retained for three (3) years for record keeping purposes. After three (3) years, it will be destroyed.

e. **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.

f. **Changes in Applicant.** An applicant with a successful Abbreviated Application may change the lead entity prior to submission of the Full Application. The applicant must provide written notice to by mail to Dr. Barbara Cuthill, NIST, MS2000, Gaithersburg, MD 20899 or by e-mail to barbara.cuthill@nist.gov in order to do so. An applicant may also revise the requested budget amount for the Full Application.

VI. Award Administration Information

1. **Award Notices.** Successful applicants will receive an award from the NIST Grants Officer. A sample award cover page, i.e., CD-450, Financial Assistance Award is available at http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/dev01_002513.pdf and the DoC Financial Assistance Standard Terms and Conditions (January 2013) are available at http://www.osec.doc.gov/oam/grants_management/policy/documents/DOC_Standard_Terms_and_Conditions_01_10_2013.pdf.

2. **Administrative and National Policy Requirements**

a. DoC Pre-Award Notification Requirements. The DoC Pre-Award Notification Requirements for Grants and Cooperative Agreements, 77 FR 74634 (December 17, 2012), are applicable to this FFO and are available at https://www.federalregister.gov/articles/2012/12/17/2012-30228/department-of-commerce-pre-award-notification-requirements-for-grants-and-cooperative-agreements.

b. Employer/Taxpayer Identification Number (EIN/TIN), Dun and Bradstreet Data Universal Numbering System (DUNS), and System for Award Management (SAM). All applicants for Federal financial assistance are required to obtain a universal identifier in the form of DUNS number and maintain a current registration in the Federal government's primary registrant database, SAM. On the form SF-424 items 8.b. and 8.c., the applicant's 9-digit EIN/TIN and 9-digit DUNS number must be consistent with the information in SAM (https://www.sam.gov/) and if applicable, the Automated Standard Application for Payment System (ASAP), if the applicant has received prior Federal awards and has received award funding through ASAP. For complex organizations with multiple EIN/TIN and DUNS numbers, the EIN/TIN and DUNS numbers MUST be the numbers for the applying organization. Organizations that provide incorrect/inconsistent EIN/TIN and DUNS numbers may experience significant delays in receiving funds if their application is selected for funding. Confirm that the EIN/TIN and DUNS number are consistent with the information on the SAM and ASAP.

Per 2 C.F.R. Part 25, each applicant must:

(1) Be registered in the CCR before submitting an application noting the CCR now resides in SAM;
(2) Maintain an active CCR registration, noting the CCR now resides in SAM, with current information at all times during which it has an active Federal award or an application under consideration by an agency; and
(3) Provide its DUNS number in each application or application it submits to the agency.

The applicant can obtain a DUNS number from Dun and Bradstreet. A DUNS number can be created within one business day. The CCR or SAM registration process may take five or more business days to complete. If you are currently registered with the CCR, you may not need to make any changes. However, please make certain that the TIN associated with your DUNS number is correct. Also note that you will need to update your CCR registration annually. This may take three or more business days to complete. Information about SAM is available at SAM.gov. *See* also 2 C.F.R. Part 25 and the *Federal Register* notice published on September 14, 2010, at 75 FR 55671.

c. 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.

d. 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, 15 C.F.R. § 14.36, and in Section B.21 of the DoC Pre-Award Notification Requirements December 17, 2012 (77 FR 74634). Questions about these requirements may be directed to the Chief Counsel for NIST, (301) 975-2803.

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.

e. 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 involving human subjects, including software testing, must meet the requirements of the Common Rule for the Protection of Human Subjects ("Common Rule"), codified for the Department of Commerce (DoC) at 15 C.F.R. Part 27. In addition, any such application that includes research activities on these topics must be in compliance with any statutory requirements imposed upon the Department of Health and Human Services (DHHS) and other Federal agencies regarding these topics, all regulatory 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 these topics.

NIST reserves the right to make an independent determination of whether an applicant's research activities involve human subjects. NIST policy also requires a NIST administrative review for research involving human subjects approved by a non-NIST Institutional Review Board (IRB). (15 C.F.R. § 27.112 Review by Institution.) If NIST determines that your application involves human subjects, you will be required to provide additional information for review and approval. If an award is issued, no research activities involving human subjects shall be initiated or costs incurred under the award until the NIST Grants Officer issues written approval. Retroactive approvals are not permitted.

NIST will accept applications that include exempt and non-exempt human subjects research activities. 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, if the application is funded. Non-exempt human subjects research activities by either domestic or foreign organizations 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 possessing 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.

The applicant should clearly indicate in the application, by separable task, all research activities believed to be exempt or non-exempt research involving human subjects and the expected institution(s) where the research activities involving human subjects may be conducted.

If an activity/task involves data obtained through intervention or interaction with living individuals or identifiable private information obtained from or about living individuals but the applicant participant(s) believes that the activity/task is not research as defined under the Common Rule, the following may be requested for that activity/task:

Justification, including the rationale for the determination and in some cases additional documentation, to support a determination that the activity/task in the application is not research as defined under the Common Rule. *See* 15 C.F.R. § 27.102. This may result in a NIST determination. If the applicant participant(s) uses a cognizant IRB that provides an IRB approval,

a copy of that IRB approval documentation will be required by NIST. The applicant participant(s) is not required to establish a relationship with a cognizant IRB if they do not have one, but if the applicant participant(s) has a cognizant IRB that requires review of the activity/task, or the applicant participant(s) elects to obtain IRB review, a copy of the IRB approval documentation will be required by NIST.

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).

a. The name(s) of the institution(s) where the exempt research will be conducted; and/or from which biological materials, or data from human subjects will be provided.
b. A copy of the protocol of 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).
c. 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.
d. Any additional clarifying documentation that NIST may request during the review process in order to make a determination that the activity or use of biological materials or data from human subjects is exempt under the Common Rule (*see* 15 C.F.R. § 27.101).

If the application appears to NIST to include research activities (exempt or non-exempt) involving human subjects, and the performer of the activity has a cognizant IRB, 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 FWAs or IRB registrations are being applied for, that should be clearly stated.

Additional documentation may be requested by NIST for performers with a cognizant IRB during review of the application, and may include the following for research activities involving human subjects that are planned in the first year of the award:

(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 may be requested;

(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.)

For more information regarding human subjects contact Linda Beth Schilling, Senior Coordinator and Policy Advisor for Human & Animal Subjects Research at NIST (e-mail: linda.schilling@nist.gov; phone: 301-975-2887).

f. Funding Availability and Limitation of Liability. Funding for the program listed in this FFO is contingent upon the availability of appropriations. In no event will NIST or DoC be responsible for application preparation costs if this program fails to receive funding or is cancelled because of agency priorities. Publication of this FFO does not oblige NIST or DoC to award any specific project or to obligate any available funds.

g. Collaborations Making Use of Federal Facilities. All applications should include a description of any work proposed to be performed using Federal facilities.

In addition, if an applicant proposes use of NIST facilities, the statement of work should include a statement of this intention and a description of the facilities. Any use of NIST facilities 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 availability of the facilities and approval of the proposed usage. Any unapproved facility use will be stricken from the application prior to the merit review. Examples of some facilities that may be available for collaborations are listed on the NIST Technology Services Web site, http://www.nist.gov/user-facilities.cfm.

h. DoC Representation by Corporations Regarding an Unpaid Delinquent Tax Liability or a Felony Conviction Under Any Federal Law. In accordance with the Federal appropriations law expected to be in effect at the time of project funding, NIST anticipates that the selected applicants will be provided a form and asked to make a representation regarding any unpaid delinquent tax liability or felony conviction under any Federal law.

3. Reporting

a. Reporting Requirements. In lieu of the reporting requirements described in Sections A.01 Financial Reports and B.01 Performance (Technical) Reports of the DoC Financial Assistance Standard Terms and Conditions dated January 2013 (http://www.osec.doc.gov/oam/grants_management/policy/documents/DOC_Standard_Terms_and_Conditions_01_10_2013.pdf), the following reporting requirements shall apply:

(1) Financial Reports. Each award recipient will be required to submit an SF-425, Federal Financial Report in triplicate (an original and two (2) copies), 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 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 in triplicate (an original and two (2) copies), 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. Two (2) copies of the technical

progress report shall be submitted to the Project Manager and the original report to the NIST Grants Officer. Technical progress reports shall contain information as prescribed in 15 C.F.R. § 14.51.

(3) Patent and Property Reports. From time to time, and in accordance with the Uniform Administrative Requirements, 15 C.F.R. Part 14 or 24, as applicable, the Department of Commerce Financial Assistance Standard Terms and Conditions dated January 9, 2013, and other terms and conditions governing the award, the recipient may need to submit property and patent reports.

b. OMB Circular A-133 Audit Requirements. Single or program-specific audits shall be performed in accordance with the requirements contained in OMB Circular A-133, "*Audits of States, Local Governments, and Non-Profit Organizations*," and the related *Compliance Supplement*. OMB Circular A-133 requires any non-Federal entity (*i.e.*, including non-profit institutions of higher education and other non-profit organizations) that expends Federal awards of $500,000 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 Circular. 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.

VII. Agency Contact(s)

Questions should be directed to the following contact persons:

Subject Area	Point of Contact
Programmatic and technical questions	Dr. Barbara Cuthill Phone: 301-975-3273 E-mail: barbara.cuthill@nist.gov
Application submission through Grants.gov	Christopher Hunton Phone: 301-975-5718 E-mail: christopher.hunton@nist.gov
Grant rules and regulations	Dean Iwasaki Phone: 301-975-8449 E-mail: dean.iwasaki@nist.gov

VIII. Other Information

Public Meeting (Applicants' Conference): NIST will hold a public meeting (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 www.nist.gov/nstic.**