April 15, 2013

ANNOUNCEMENT OF FEDERAL FUNDING OPPORTUNITY (FFO)
National Strategy for Trusted Identities in Cyberspace (NSTIC) Pilots: Trusted Online Credentials for Accessing Government Services
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: Trusted Online Credentials for Accessing Government Services Cooperative Agreement Program

- **Announcement Type:** Initial

- **Funding Opportunity Number:** 2013-NIST-NSTIC-02

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

- **Dates:** Electronic applications must be received no later than 11:59 p.m. Eastern Time, Thursday, May 16, 2013. Applications received after this deadline will not be reviewed or considered. The earliest anticipated start date for awards under this FFO is expected to be August 1, 2013.

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

- **Funding Opportunity Description:** NIST invites applications from eligible applicants to pilot on-line identity solutions for accessing government services 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 the effectiveness of solutions for enabling individuals to better access government services that either do not exist or are not widely adopted in the marketplace today. To demonstrate that the solution meets the program's goals, NSTIC will be looking for the following characteristics in applications:

  i. At least two government programs, including state-administered human services programs, which will use the trusted credential;
  ii. A private provider to be used to supply at least part of the identity credential; and
  iii. Information on why the planned solution is replicable elsewhere.

  See section V.3 Initial Administrative Review for further discussion of the review of this information.

- **Funding Availability**. NIST anticipates that awards will be in the range of approximately $1,250,000 for one year. Proposed funding levels must be consistent with project scope. NSTIC will consider applications with lower funding amounts. The number of projects funded will depend on the amount

of available funds. The maximum possible for new awards is not expected to exceed $2.7 million. Funds for the program are provided to NIST from the Office of Management and Budget's Partnership Fund for Program Integrity Innovation.

- **Funding Instrument:** Cooperative agreement.

- **Who Is Eligible:** State, local, and Indian tribal governments located in the United States and its territories and non-profit organizations. An eligible organization may work individually or include proposed subawardees, contractors or other collaborators in a project proposal, effectively forming a team or consortium. In a team or consortium, eligible subawardees are U.S. non-profit organizations, accredited institutions of higher education, commercial organizations, and state, tribal, and local governments. 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 plans to hold an Applicants' Conference to offer **general** guidance on preparing applications, and to answer questions. Attendance at an NSTIC Applicants' Conference is **not required. Information on the Applicant's Conference is available at http://www.nstic.gov.**

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), and (c)(12), and P.L. 111-117 and P.L. 112-74.

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.

The 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. 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."

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.

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 and state and local government 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; 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. NIST also funded five (5) pilot projects in the initial round of NSTIC pilots cooperative agreements.

In implementing the Strategy, the NSTIC NPO seeks to promote the existing marketplace, encourage new solutions, and establish a baseline of privacy, security, interoperability, and ease of use that will enable the market to flourish.

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

Pilots Program Focus Area: Trusted Online Credentials for Accessing Government Services

The purpose of the NSTIC Trusted Online Credentials for Accessing Government Services 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., they will test or demonstrate new solutions, models and frameworks that either do not exist or are not widely adopted today).

As state and local governments increasingly shift eligibility and enrollment processes for services to a virtual environment, they are challenged to develop effective and secure identity verification solutions to support convenient customer access and program integrity across different services and agencies. The proposed pilots would alleviate this challenge by providing competitive grants to agencies or non-profits to enable multiple human services programs to use trusted online credentials that meet the Strategy's four Guiding Principles.

According to the Federal Trade Commission's Consumer Sentinel Network Data Book for January-December 2011, identity theft to obtain government documents or benefits accounted for 27% of all identity theft complaints in 2011. Specific examples cited by states participating in OMB's Collaborative Forum include:

1. Florida's active Medicaid eligibility error rate reported by the Centers for Medicare and Medicaid (CMS) is 9.2%. The Corrective Action Plan issued in response to the CMS audit review concluded that improper identity verification was a root cause of the eligibility error rate.
2. The Florida Department of Children and Families (DCF), the agency responsible for Medicaid and other public assistance programs, further analyzed eligibility errors and fraud for Medicaid and the Supplemental Nutrition Assistance Program (SNAP) based on a sample analysis performed in September 2011. Based on the sample results, 2.8% of Medicaid and 6.29% of SNAP eligibility errors were related to identity fraud or $3,670,593 and $6,320,500 of the payment errors, respectively.
3. Kansas' Department of Social and Rehabilitation Services conducted a state review of SNAP in October 2011 and found 312 possibly dead recipients, 941 cases in which there was severe risk of identity fraud, 261 recipients believed to be incarcerated, and 6,400 who had out-of-state driver's licenses.

Identity issues present major challenges to public benefits programs and many past efforts to address these challenges have failed to gain significant traction due to a number of barriers, including:

1. Concerns about applicant and beneficiary privacy, such as concerns that identity proofing techniques may be too intrusive, as well as concerns that data collected will be inappropriately shared with other programs or parties.

2. Difficulties conducting identity proofing and ensuring that commonly-used identity proofing approaches can adequately cover 100% of the beneficiary population.

3. The high per-user costs of many identity solutions, some of which even exceed the budgets of agencies, particularly when the solution would only be used in a single service, as well as

challenges demonstrating the ability to show how costs could be recovered.

4. Security challenges faced by some states in demonstrating an ability to securely store sensitive information.

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 NSTIC's four guiding principles and complements other NSTIC Identity Ecosystem pilots efforts. The projects can thus provide a foundation upon which the Identity Ecosystem can be constructed for improvement of public benefits administration, specifically of identity verification in both online application for government benefits and the electronic provision of those benefits.

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

1. By leveraging new privacy-enhancing technologies (PETs), such as zero-knowledge encryption, identity solutions that would share the minimal amount of data needed to enable the validation of specific attributes necessary to complete an application or transaction. Sensitive information would not be unnecessarily shared or aggregated, addressing security and privacy concerns.

2. Existing identity proofing solutions in the Identity Ecosystem could be leveraged and re-used rather than require applicants and beneficiaries to start from scratch.

3. For services requiring a secure credential for access – rather than issue a new credential specific to that service, an existing credential accredited for use in the Identity Ecosystem could be re-used.

Priority will be given to projects which 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.

Note that while the solutions may be vendor supplied proprietary solutions, NIST requires that the solutions be interoperable within the Identity Ecosystem and not lock the applying agency or non-profit into a single solution. The pilots would have to demonstrate that the approach could be replicated across multiple agencies, programs and jurisdictions.

These pilots would also complement similar Partnership Fund pilot efforts in addressing identity verification at the start of the program application and eligibility processes and in continuing accuracy of the electronic provision of those benefits. Pilots underway are targeting eligibility and enrollment decisions in SNAP, Medicaid, and other human services programs. NSTIC would consider pilots that use trusted online identity credentials compliant with NSTIC guiding principles to improve this decision-making.

Project participants (the project lead, contractors, subawardees and other collaborators) must possess the education, experience, and training to pursue and advance implementation of the 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 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. **Funding Availability.** NIST anticipates that awards will be in the range of approximately $1,250,000 for one year. Proposed funding levels must be consistent with project scope. NSTIC will consider applications with lower funding amounts. The number of projects funded will depend on the amount of available funds. The maximum possible for new awards is not expected to exceed $2.7 million. Funds for the program are provided to NIST from the Office of Management and Budget's Partnership for Program Integrity Innovation.

III. Eligibility Information

- **Eligible Applicants**. State, local, and Indian tribal governments located in the United States and its territories and non-profit organizations. An eligible organization may work individually or include proposed subawardees, contractors or other collaborators in a project proposal, effectively forming a team or consortium. In a team or consortium, eligible subawardees are U.S. non-profit organizations, accredited institutions of higher education, commercial organizations, and state, tribal, and local governments. Federal agencies may participate in projects but may not receive NIST funding.

- **Cost Sharing or Matching**. Cost sharing and matching are not required under this Program.

IV. Application/Proposal and Submission Information

1. **Address to Request Application Package.** The standard application package, consisting of the standard forms, i.e., SF-424, SF-424A, SF-424B, SF-LLL, and the CD-511, is available at www.grants.gov. The standard application package may be requested by contacting the NIST personnel listed below:

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

2. **Content and Format of Application/Proposal Submission**

a. **Required Forms and Documents**

   (1) SF-424, Application for Federal Assistance. The SF-424 must be signed by an authorized representative of the applicant organization. The FFO number 2013-NIST-NSTIC-02 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
   (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, consistent with the evaluation criteria (*see* Section V.1. of this FFO). The executive summary should include information indicating how each evaluation criteria and its sub-factors are addressed. A table can be helpful in providing this information. The executive summary should not exceed two (2) pages.

(b) Project Approach. A description of the proposed approach, sufficient to permit evaluation of the application 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 can be used to present this information. This section should be the primary, but not only, means by which the application will be evaluated according to the *Adherence to the NSTIC Guiding Principles* evaluation criterion (*see* Section V.1. of this FFO).

(c) Statement of Work and Implementation Plan. A statement of work that discusses the specific tasks proposed to be carried out, 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 schedule of tasks and events can be presented as a Gantt Chart, Work Breakdown Structure (WBS) or other format. (Note that the Gantt Chart, Work Breakdown Structure or other planning documents are outside the page count.) This section should be the primary, but not only, means by which the application will be evaluated according to the *Quality of the Implementation Plan* evaluation criterion (*see* Section V.1. of this FFO).

(d) Project Impact. A description of how the project will promote goals of the Partnership Fund outlined in the evaluation criteria, including improving program integrity and efficiency as well as convenient customer access across programs and agencies. In addition, this section should describe plans to scale the pilot project into full production including the ongoing role of all the organizations involved in the project in the Identity Ecosystem. This section should be the primary, but not only, means by which the application will be evaluated according to the *Contribution to the Identity Ecosystem* evaluation criterion (*see* Section V.1 of this FFO).

(e) Qualifications. A description of the qualifications and proposed role of each project participant, including the proposed role of the project lead and of each subwardee, contractor, or other collaborator;, and planned use of NIST funds. In addition, this section should include a description of the qualifications, including skills and experience and role of all key personnel on the project. This section and the budget narrative should be the primary, but not only, means by which the application will be evaluated according to the *Resource Availability* evaluation criterion (*see* Section V.1. 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 hours or effort level), salary rate, and 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 - For travel costs requested in the application, the budget justification 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. 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.

(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. Successful applicants will be required to obtain such a rate.

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.(8) 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.

b. 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.

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; Gantt Chart or Work Breakdown Structure or other planning document (if included); Budget Narrative; and Indirect Cost Rate Agreement.

(7) Page numbering. Number pages sequentially.

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

(9) Language. English.

3. Submission Dates and Times. Applications must be received by NIST no later than 11:59 p.m. Eastern Time, Thursday, May 16, 2013 via the Grants.gov website. Applications received after the 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 early.

In the event of a natural disaster that interferes with timely application submissions, NIST may issue an amendment to this FFO to change the application due date.

4. Intergovernmental Review. Proposals 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 2013-NIST-NSTIC-02.

(1) Applicants 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 2013-NIST-NSTIC-02 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) Information essential to successful application submission on the Grants.gov system is detailed in the For Applicants section found in red on the left side of the www.grants.gov home page, and all potential applicants should pay close attention to the information contained therein. The All About Grants, Applicant FAQs, and Submit Application FAQs sections found under the Applicant Resources option are particularly important.

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/Proposal Review Information

1. Evaluation Criteria. The evaluation criteria that will be used in evaluating applications are as follows:

A. Adherence to NSTIC Guiding Principles (0 - 30 points, sub-criteria a. through e. below receive equal weight):

a. Privacy-enhancing and voluntary – The envisioned Identity Ecosystem will mitigate privacy and civil liberties risks engendered by the capability for greater identification, tracking, and personal data aggregation. Such mitigation will be grounded in conformance to the Fair Information Practice Principles (FIPPs) (see Appendix A of NSTIC) 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. 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:

I. How the application:

1. Addresses any collection, use, and disclosure or transmission of personal information;
2. 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;
3. 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;
4. Minimizes retention of personal information;
5. Minimizes data aggregation and linkages across transactions;

6. Provides appropriate mechanisms to allow individuals to access, correct, and delete personal information;
7. Establishes accuracy standards for personal information used in identity assurance, authentication or authorization solutions;
8. Protects, transfers at the individual's request, and securely destroys personal information when terminating business operations or overall participation in the Identity Ecosystem;
9. Accounts for how personal information is actually collected, used, disclosed or transmitted and retained, and provides mechanisms for compliance, audit, and verification; and
10. Provides effective redress mechanisms for, and advocacy on behalf of, individuals who believe their personal information may have been misused.

II. 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; which project participant(s) will be responsible for the implementation; and supporting performance metrics for such implementations; and

III. Describing what role, if any, trust frameworks will play in the enforcement of a common privacy framework applicable to all project participants, including identity providers (IdPs and relying parties(RPs).

b. 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.

c. 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. For instance, if the entity supplying the credential is the only entity accepting the credential then interoperability has not been demonstrated.

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.

d. 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 (i.e., 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 the 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.

e. Integration of all Four Principles – Identity solutions should demonstrate that they implement all four guiding principles (a. through d. above) in an integrated manner.

B. Contribution to Identity Ecosystem (0 - 15 points)

Identification of how the proposed trusted identity solution will move beyond the pilot phase to contribute more broadly to the Identity Ecosystem. Making this transition includes the ease with which the solution could be implemented elsewhere.

Reviewers will be looking for details on:

- The potential number of end users in the proposed project, for example, the number of credentials issued or the number of anticipated RPs.
- The ability of the proposed project to develop new or strengthen existing digital identity services.
- The reliance on new or existing Trust Frameworks to accomplish project objectives.
- The ability of the proposed project to contribute to the development of the Identity Ecosystem Framework.
- The plan for scaling beyond the proposed pilot and expanding beyond any initial proprietary solution.
- The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into production and to replicate the pilot elsewhere..
- How the applicant intends to interact and engage with the Identity Ecosystem stakeholders to ensure transparency and visibility within the Identity Ecosystem.

C. Measurable Outcomes and Impacts (0 - 30 points). Identification of how the proposed trusted identity solution when implemented by the services identified in the application would improve two or more of the following service outcomes and how that impact could be measured:

1. Improving program integrity

2. Improving administrative efficiency
3. Improving service delivery
4. Reducing access barriers for beneficiaries

Applicants are expected to identify cost savings and other quantified targets for measuring the performance of the proposed project against at least two of these outcomes as well as available data sources that will be used to track performance.

D. Quality of Implementation Plan (0 - 15 points)

Quality of the applicant's plans for implementation includes tasks, schedule, quantified objectives, metrics, method of measuring the metrics, milestones, risks, and plans for stakeholder outreach and integration with other efforts.

Reviewers will be looking for details on:

- Milestones that allow assessment of incremental progress and fit into the overall schedule.
- Sufficient detail around tasks and activities that clearly reflect implementation of the proposed project objectives and scope of work.
- An understanding of key project risks and risk response strategies.
- Alignment of proposed performance metrics with project objectives, NSTIC Guiding Principles and soundness of proposed measurement approach.
- The roles of all project participants.

E. Resource Availability (0 - 10 points)

Reviewers will be looking for details on:

- The applicant's ability to commit quality resources to the project, including the qualifications and commitment of the identified project participants, and previously demonstrated ability to achieve positive outcomes in similar endeavors.
- The appropriateness of proposed resources compared to the project's scope, as well as the cost-effectiveness of the project in using available resources to complete the project.
- The plan to obtain or leverage additional or external resources to engage in post-project commercialization and move the project results into routine use.

2. Selection Factors. The Selecting Official, who is the Senior Executive Advisor for Identity Management, shall select applications for award based upon the ranking and 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 of states involved in the pilots.

d. Diversity of technical approaches across all funded projects to providing a foundation for the Identity Ecosystem.

e. Diversity in the applications addressed by the funded projects.

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

3. Review and Selection Process

- **Initial Administrative Review.** An initial review of timely received applications will be conducted to determine eligibility, completeness, and responsiveness to this FFO and the scope of the stated program objectives. Responsiveness requires that the applicant identify in the application:

  i. At least two (2) government programs which will use the trusted credential, including state-administered human services programs, ;
  ii. A private provider to be used to supply at least part of the identity credential; and
  iii. Information on why the planned solution is replicable elsewhere.

  Applications determined to be ineligible, incomplete, and/or non-responsive may be eliminated from further review.

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

  Each application will be reviewed by at least three (3) independent, objective reviewers, 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.

  An Evaluation Board, a committee comprised of Federal employees, will consider the reviewers' written evaluations based on the evaluation criteria (see Section V.1.of this FFO). The Evaluation Board may ask questions of some or all applicants in writing and/or may require teleconferences with some or all applicants. Any teleconferences are expected to occur in mid-June 2013. Applicants may also be asked to provide from potential project participants at this time. Using the additional information and the technical review comments and scores, the Evaluation Board will prepare a final ranking of the applications. These applications and rankings will be forwarded to the Selecting Official for further consideration.

  In making final selections, the Selecting Official will select funding recipients based upon the Evaluation Board's ranking of the applications and the selection factors (see Section V.2. of this FFO).

  In accordance with the Federal appropriations law expected to be in effect at the time of project funding, NIST anticipates that the selected applicant will be provided a form and asked to make a representation regarding any unpaid delinquent tax liability or felony conviction under any Federal law.

  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 and selection of successful applicants, and award processing is expected to be completed in July 2013. The earliest anticipated start date for awards made under this FFO is expected to be August 1, 2013.

5. Additional Information

a. 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 by the submission deadline via Grants.gov.

b. Program Evaluation. NSTIC 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.

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

d. Retention of Unsuccessful Applications. An electronic copy of each non-selected 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.

VI. Award Administration Information

1. Award Notices. Successful applicants will receive an award from the NIST Grants Officer. The 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 Automated Standard Application for Payment System (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 a 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 a application under consideration by an agency; and
(3) Provide its DUNS number in each 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 Projects Involving Human Subjects, Human Tissue, Data or Recordings Involving Human Subjects Including Software Testing. Any application that includes research involving human subjects, human tissue/cells, 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 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 involves human subjects. If NIST determines that your research project 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. Non-exempt human subjects research activities will be required to have protocols approved by an Institutional Review Board (IRB) currently registered with the Office for Human Research Protections (OHRP) within the DHHS and that will be performed by entities possessing a currently valid Federal-wide Assurance (FWA) on file from OHRP that is appropriately linked to the cognizant IRB for the protocol. Information regarding how to apply for an FWA and register and IRB with OHRP can be found at http://www.hhs.gov/ohrp/assurances/index.html. ***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.***

Generally, NIST does not fund research involving human subjects in foreign countries. NIST will consider, however, the use of **preexisting** tissue, cells, or data from a foreign source on a limited basis if all of the following criteria are satisfied:

(1) the scientific source is considered unique,
(2) an equivalent source is unavailable within the United States,
(3) an alternative approach is not scientifically of equivalent merit, and
(4) the specific use qualifies for an exemption under the Common Rule.

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 project participant 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 project is not research as defined under the Common Rule. *See* 15 C.F.R. 27.102. Some cases may result in a NIST determination or an applicant or recipient may choose to provide an IRB approval (if the project participant uses a cognizant IRB).

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 project participant believes that the task/activity is not research as defined under the Common Rule, the following will be required for that activity/task:

> Documentation or an IRB approval (if the project participant has a cognizant IRB), including the rationale for the determination, to support a determination that the activity/task in the project is not research as defined under the Common Rule [see 15 C.F.R. 27.102].

If the application appears to include research activities involving human subjects 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, as warranted, during review of the application, but 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 applicable to 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 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.

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

g. 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.

h. 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 Web site, http://www.nist.gov/user-facilities.cfm.

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. 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)

Subject Area	Point of Contact
Programmatic and technical questions	Dr. Barbara Cuthill Phone: 301-975-3273 E-mail: barbara.cuthill@nist.gov
Electronic submission through Grants.gov	Christopher Hunton Phone: 301-975-5718 Fax: 301-840-5976 E-mail: christopher.hunton@nist.gov
Grant rules and regulations	Debbie Chen Phone: 301-975-6646 Fax: 301-840-5976 E-mail: debbie.chen@nist.gov

Research projects involving human subjects, human tissue, data or recordings involving human subjects including software testing	Linda Beth Schilling Phone: 301-975-2887 E-mail: linda.schilling@nist.gov

VIII. Other Information

Public Meetings (Applicants' Conference): NIST plans to hold a public meeting (Applicants' Conference), to offer general guidance on preparing applications, and to answer questions. The Applicant's Conference will be webcast. Attendance at an NSTIC Applicants' Conference is **not required. Information on the Applicant's Conference is available at http://www.nstic.gov .**