March 26, 2015

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

- **Announcement Type:** Initial

- **Funding Opportunity Number:** 2015-NIST-NSTIC-02

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

- **Dates:** Applications must be received electronically through Grants.gov no later than 11:59 p.m. Eastern Time, Thursday, May 28, 2015. Applications received after this deadline will not be reviewed or considered. NIST expects to complete review of Applications, selection of successful applicants, and award processing in September 2015. The earliest anticipated start date for awards under this FFO is expected to be September 2015.

  Keep in mind when developing your submission timeline the following:

  1) In order to register in Grants.gov, your organization must have a current registration in the System for Award Management (SAM) (*see* Section IV.3. of this FFO). The registration process in SAM may take more than two weeks. Note that SAM requires annual registration renewal.

  2) Applicants using Grants.gov will receive email notifications over a period of up to two business days as the application moves through intermediate systems before the applicant learns via a validation or rejection notification whether NIST has received the application.

- **Application Submission Address:** Applications will only be accepted using Grants.gov**.**

- **Funding Opportunity Description:** NIST is soliciting applications from eligible applicants to pilot privacy-enhancing technologies that embrace and advance the NSTIC vision and contribute to the maturity of the identity ecosystem the NSTIC

envisions: Promote secure, user-friendly ways to give individuals and organizations confidence in their online interactions. 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 demonstrate or deploy new solutions 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 $750,000 to $1,500,000 per year per project for up to two 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. NIST anticipates funding new pilots with total funding of up to approximately $2.5 million.

- **Funding Instrument:** Cooperative agreement.

- **Who Is Eligible:** Accredited institutions of higher education; non-profit organizations; and commercial organizations incorporated in the United States; and state, local, territorial and Indian tribal governments within the United States. While a non-governmental applicant must be incorporated in the United States, the applicant may have a parent organization outside the United States. 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 (Webinar):** NIST will hold a webinar 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 webinar or at any time before submitting the application to NIST. Also, NIST/NSTIC Program Office staff will not critique or provide feedback on project ideas while they are being developed by an applicant. Attendance at the Webinar is **not required. Information on the Webinar is available at www.nist.gov/nstic.**

Table of Contents

FULL ANNOUNCEMENT TEXT

I. Program Description

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

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

The Strategy'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 data that are improperly disclosed or unnecessarily aggregated, 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-identified 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;

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

- **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.

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

NIST Funded Projects Advancing the NSTIC Strategy

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

NIST began funding pilot projects under the NSTIC Pilot Cooperative Agreement Program in 2012 and has made awards under this program in each of the subsequent years. NIST funded five pilot projects in the initial round of the NSTIC Pilots Cooperative Agreement Program in 2012. In 2013, NIST funded five additional pilot projects in the program's second round. In 2014, NIST funded three additional pilot projects under the program. Descriptions of the pilot projects funded in the past are available on the NSTIC website at http://www.nist.gov/nstic/pilot-projects.html. Earlier in 2015, NIST posted an FFO announcing the availability of funding for a fourth round of pilots; awards are expected to be made in September 2015. NIST is now posting this FFO, announcing the availability of funding for pilots with a special focus on privacy enhancing technologies.

To further advance the development of the Identity Ecosystem Framework and to build on the existing marketplace in online credentials, NIST has provided financial assistance to the Identity Ecosystem Steering Group (IDESG). The IDESG is the only

private sector organization currently committed to developing the Identity Ecosystem Framework. More information on the IDESG is available at http://www.idecosystem.org.

Privacy Pilots Program Focus Area: Building Privacy-Enhancing Technologies into Federated Identity Solutions

The purpose of the NSTIC Privacy 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 projects will deploy pilots to test or demonstrate new solutions 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 that include real users conducting real transactions with real data.

The identity solutions marketplace has particularly struggled with the privacy-enhancing guiding principle of the NSTIC. This guiding principle is intended to address concerns that the development of more trusted and federated identity solutions could create risks for privacy and civil liberties, including risks that arise from the crossing of contextual boundaries (e.g., risks to privacy created by entities in different sectors linking individuals' transactions) and the capacity for more tracking and profiling of individuals.

Although risks can be mitigated through the implementation of policy and technical controls, the selection of the type of control should rest on a risk assessment that includes a determination of which type of control would be most effective. Market forces alone have not balanced these choices as, to date, mitigations have been weighted towards policy controls even though, in many cases, privacy-enhancing technologies or architectural design choices could be used to more effectively mitigate privacy or civil liberties risks. Barriers exist to the implementation of privacy-enhancing technologies, especially cryptographic-based technologies, which hold the promise to substantially reduce privacy risk. These barriers may arise from a lack of: protocols or standards for deployment of privacy-enhancing technologies that can be readily integrated with existing technologies in the marketplace; awareness that specific technologies exist and the types of risks these technologies can effectively mitigate; usability of these technologies; and/or demonstrated proof of performance and scalability. Thus, the NSTIC NPO is interested in funding projects (i) with innovative approaches to overcoming these barriers; (ii) that align with all four of NSTIC's guiding principles while providing practical, market-ready solutions; and (iii) that appropriately balance policy and technical controls to mitigate specific identified privacy or civil liberties risks.

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

- Create and demonstrate technical standards or solutions for enabling the exchange of specific attributes associated with identities while minimizing the disclosure of incidental or non-operational personal information[2], including:
    - Operational technical standards or protocols to obscure intermediaries' visibility into the identity attributes being shared in the online transactions they are facilitating;
    - Technology architectures, software developer kits, or application programming interfaces that offer sufficiently granular management of personal information, either by participating entities or individuals;
    - Offer the opportunity for relying parties to receive claims of attribute validity instead of disclosing all or part of an attribute's value.
- Solve contextual boundary concerns that discourage user adoption of federated identity solutions such as blinding identity providers from relying parties, and vice versa.
- Improving the usability of privacy enhancing technologies, especially in establishing user understanding of what is occurring with user data.
- Balancing transparency to individual users and ease-of-use.
- Technical standards for managing meaningful consent.

.
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 as well as the project goals and objectives. Project participants should demonstrate the strength of the partnership and highlight any prior collaborations. Particular attention will be given to projects that can be feasibly deployed into the marketplace by the end of pilot program, including support of viable business models, current security requirements, and generally accepted performance standards, and use existing standards and protocols deployed or configured in innovative ways to address the privacy or civil liberties risks.

II. Federal Award Information

1. **Funding Instrument.** The funding instrument that will be used is a cooperative agreement. The nature of NIST's "substantial involvement" 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://go.usa.gov/SNJd. Please note the DoC Grants and Cooperative Agreements Manual is expected to be updated after publication of this funding announcement and before October 1, 2015. Refer to Section VII. of this FFO, Agency Contacts,

[2] Personal information is any information, including behavioral information, about or that can be associated with individuals.

Grant Rules and Regulations, if you seek the information at this link and it is no longer working or you need more information

2. **Multi-Year Funding Policy.** When an application for a multi-year award is approved, funding will usually be provided for only the first year of the project. If a project is selected for funding, NIST has no obligation to provide any additional funding 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 $750,000 to $1,500,000 per year per project for up to two 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. NIST anticipates funding new pilots with total funding of up to approximately $2.5 million.

III. Eligibility Information

1. **Eligible Applicants.** Accredited institutions of higher education; non-profit organizations; and commercial organizations incorporated in the United States; and state, local, territorial and Indian tribal governments within the United States. While a non-governmental applicant must be incorporated in the United States, the applicant may have a parent organization outside the United States. 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.

IV. Application Submission Information

1. **Address to Request Application Package.** The application package is available at www.grants.gov. Applicants may also request an application package by contacting the point of contact for Programmatic and Technical Questions listed in Section VII. of this FFO.

2. **Content and Form of Application Submission**

a. **Required Application Forms and Documents**

The following are required for a complete application:

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

SF-424, Item 12, must list the FFO number 2015-NIST-NSTIC-02.

SF-424, Item 18, must list the total budget information for the duration of the project for multi-year applications.

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 20 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 Privacy Enhancing Technology Deployed. A problem statement that discusses the barrier(s) or challenge(s) to the implementation of the NSTIC privacy guiding principle and a description of the privacy enhancing technology that will address those barriers. Be clear about what this project would fund that otherwise would not happen. If the proposed project addresses barrier(s) or challenge(s) to the

implementation of the NSTIC privacy guiding principle 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 a general description of the privacy enhancing technology deployed in the proposed pilot, as well as a technical description of the approach to deploying this technology. This should include the core properties achieved by the technology, and standards and protocols employed by the technology. In addition, this section should discuss which project participant(s) will be responsible for the implementation of the privacy controls; what supporting metrics will be used to measure these controls; and, to the extent that the solution provides control points for individuals to manage their personal information, how such control points are designed to enable individuals to effectively mitigate privacy risks.

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

(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 use cases, operational requirements that the solution implements, 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. Information on the use cases should include what use cases will actually be demonstrated during the proposed project and why those use cases were chosen. An architecture diagram and data flow diagrams, including data flows among project participants, can be used to present this information and will not be counted within the page limit. The applicant should provide information on what needs to be done to initiate the pilot, complete the pilot, and evaluate the pilot. 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 identify which privacy and civil liberties risks are being mitigated (such as those arising from the capability for greater identification, tracking or linkability of transactions, or personal data

aggregation), and how the solution mitigates such risks. The applicant must clearly state where the solution enforces privacy and civil liberties protections by either (or both) technical and policy means, the expected effectiveness of such controls and any trade-offs made between the selection of policy and technical controls. This section should explain how the technical and/or policy measures are applied in a risk-based approach to identified privacy risks.

All aspects discussed as part of the solution should be included in the description of the operational pilot. The detailed analysis of the identified privacy risks and how the solution is designed to mitigate them (e.g., using the Privacy Evaluation Methodology (PEM) (see https://www.idecosystem.org/content/pem-archive) or an analysis against NIST's privacy risk management approach (see http://csrc.nist.gov/projects/privacy_engineering/documents.html)) should be presented as a separate document. See the NIST Privacy Engineering website at http://csrc.nist.gov/projects/privacy_engineering/index.html for more information on this approach. (Note that this document with a detailed analysis of identified privacy risks and how the solution is designed to mitigate them is not counted within the page limit.)

This section and the previous 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 complete statement of work covering all project participants that includes the following:

- The specific proposed tasks,
- 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 project leadership's plans to oversee all project participants, including sub-recipients, contractors etc. to ensure realization of project goals and objectives,
- The approach to ensure the project results will align to all four NSTIC guiding principles,
- Realistic, measurable milestones tied to metrics for the entire project, demonstrating progress in all areas relevant to the overall pilot.

All aspects discussed as part of the solution should be included in the implementation plan and have associated milestones. 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.) Letters of commitment from project participants

should reference the expected role and level of effort in the statement of work.

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

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

(f) Qualifications. A description of the qualifications 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. Include past experience collaborating with others on the team or in similar collaborations, if applicable.

All participating organizations are expected to identify at least one key person and that person's time commitment to the project. The key personnel for the overall project should include the following:

- At least one individual from each participant, with details of committed participation, provided.
- A project manager or project leader with demonstrated experience leading projects of similar size and complexity and previously demonstrated ability to achieve positive outcomes in pilot programs and similar endeavors.
- At least one privacy engineer with specialized knowledge of both privacy technology and policy issues is expected on all projects. This individual(s) will be considered key to the project and shall ideally have at least 5-7 years' experience in a cross-set of privacy and information technology skills. This individual may be an employee of the applicant, or he or she may be a consultant or employee of a contractor or subawardee. Although less preferable, this role could be filled by multiple individuals with complementary skillsets and experience. Experience may be demonstrated by education, certifications, and job skills. Qualifications for the privacy skillset could include certifications such as CIPT or CIPM and experience implementing privacy principles such as the Fair Information Practice Principles, identifying and mitigating privacy risks in the implementation of information technology systems. Qualifications for the technical skillset could include advanced

degrees in computer science, information science, or computer engineering and experience with architectural design for information systems; data, systems, or software engineering; and related aspects of technical privacy implementations. If multiple individuals are used to meet this qualification, the applicant must include a description of how the multiple individuals will work together to compensate for the lack of the combined skillset in a single individual.

- At least one subject matter expert in usability of the type of system envisioned for the project.

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

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

(7) Budget Narrative. The Budget Narrative should provide a detailed breakdown of each of the object class categories as reflected on the SF-424A. The budget justification should address all of the budget categories (personnel, fringe benefits, equipment, travel, supplies, other direct costs and indirect costs). The written justification should include the necessity and the basis for the cost. Only allowable costs should be included in the budget. Information on cost allowability is available in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200, which apply to awards in this program. More information is available at http://go.usa.gov/SBYh and http://go.usa.gov/SBg4. 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 goods and services. Subawardees perform part of the project scope of work. For each subaward, applicants must provide budget detail justifying the cost of the work performed on the project.

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

(8) Indirect Cost Rate Agreement. If indirect costs are included in the proposed budget, provide a copy of the approved negotiated agreement if this rate was negotiated with a cognizant Federal audit agency. If the rate was not established by a cognizant Federal audit agency, provide a statement to this effect. If the successful applicant includes indirect costs in the budget and has not established an indirect cost rate with a cognizant Federal audit

agency, the applicant will be required to obtain such a rate in accordance with Section B.06 Indirect or Facilities and Administrative Costs of the Department of Commerce Financial Assistance Standard Terms and Conditions (December 26, 2014), available at http://go.usa.gov/hKbj .

(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, including relying parties, 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 and the level of organizational commitment to the project. A letter is required whether or not the organization is receiving Federal funds. Note that the letters of commitment are part of the material addressing *Resource Availability* evaluation criterion (*see* Section V.1.d of this FFO).

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

(10) **Resumes of Key Personnel including Privacy Expert(s).** Resumes of all key personnel including the project's privacy expert(s) are required. These resumes are to be a maximum of two pages each. Additional pages beyond the two per resume will not be considered. Note that the resumes are part of the material addressing *Resource Availability* evaluation criterion (*see* Section V.1.d of this FFO).

Items IV.2.a.(1) through IV.2.a.(5) above are part of the standard application package in Grants.gov and can be completed through the download application process. **Items IV.2.a.(6) through IV.2.a.(10) must be completed and attached by clicking on "Add Attachments" found in item 15 of the SF-424, Application for Federal Assistance. This will create a zip file that allows for transmittal of the documents electronically via Grants.gov.**

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

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.

(7) **Page Limit.** The Technical Proposal for Applications is limited to 20 pages.

Page limit includes: Table of contents (if included), Technical Proposal, 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); detailed analysis of the identified privacy risks and how the solution is designed to mitigate them (e.g., using the Privacy Evaluation Methodology (PEM) (*see* Section IV.2.a.(6)(c) of this FFO and *see also* https://www.idecosystem.org/content/pem-archive) or an analysis against NIST's privacy risk management approach (see http://csrc.nist.gov/projects/privacy_engineering/documents.html)) ; Budget Narrative; and Indirect Cost Rate Agreement; letters of interest and letters of commitment; and resumes.

(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.

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

d. **Pre-Applications.** NIST is not accepting pre-applications or white papers under this FFO.

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

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

4. **Submission Dates and Times.** Applications must be received electronically through Grants.gov no later than 11:59 p.m. Eastern Time, Thursday, May 28, 2015. Applications received after this deadline will not be reviewed or considered. Review of applications, selection of successful applicants, and award processing is expected to be completed in September 2015. The earliest anticipated start date for awards under this FFO is expected to be September 2015.

   Applications not received by the specified due date and time will not be considered and will be returned without review. NIST will consider the date and time stamped on the validation generated by www.grants.gov as the official submission time.

   NIST will not accept applications submitted by mail, facsimile, or email.

   NIST strongly recommends that applicants do not wait until the last minute to submit an application. NIST will not make any allowances for late submissions resulting from an applicants' inability to register with Sam.gov or Grants.gov in a timely manner. The responsibility for ensuring a complete application is received by NIST

by the deadline is the sole responsibility of the applicant. To avoid any potential processing backlogs due to last minute Grants.gov registrations, applicants are strongly encouraged to start their Grants.gov registration process at least four (4) weeks prior to the application due date.

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 IV.3. of this FFO) may take between three and five business days or as long as 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 whether a Federal agency's electronic system has received its application.

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

6. **Funding Restrictions.** Profit or fee is not an allowable cost.

7. **Other Submission Requirements**

a. Applications must be submitted electronically through www.grants.gov . NIST will not accept applications submitted by mail, facsimile, or e-mail.

(1) Electronic applications must be submitted via Grants.gov at www.grants.gov, under announcement 2015-NIST-NSTIC-02.

a) Applicants should carefully follow specific Grants.gov instructions to ensure that all attachments will be accepted by the Grants.gov system. A receipt from Grants.gov indicating an application is received does not provide information about whether attachments have been received. For further information or questions regarding applying electronically for the 2015-NIST-NSTIC-02 announcement, contact Christopher Hunton by phone at 301-975-5718 or by e-mail at christopher.hunton@nist.gov.

b) Applicants are strongly encouraged to start early and not wait until the approaching due date before logging on and reviewing the instructions for submitting an application through Grants.gov. The Grants.gov registration process must be completed before a new registrant can apply electronically. If all goes well, the registration process takes three (3) to five (5) business days. If problems are encountered, the registration process can take up to two (2) weeks or more. Applicants must have a valid unique entity identifier number and must maintain a current registration in the Federal government's primary registrant database, the System for Award Management (https://www.sam.gov/), as explained on the Grants.gov Web site. *See also* Section IV.3. of this FFO. After registering, it may take several days or longer from the initial log-on before a new Grants.gov system user can submit an

application. Only 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.

c) To find instructions on submitting an application on Grants.gov, Applicants should refer to the "Applicants" tab in the banner just below the top of the www.grants.gov home page. Clicking on the "Applicants" tab produces the "Grant Applicants" page.

    a. 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.

    b. 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.

    c. 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.

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

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

b. Amendments. Any amendments to this FFO will be announced through Grants.gov. Applicants may sign up for Grants.gov FFO amendments or may

request copies from Dr. Barbara Cuthill by telephone at (301) 975-3273 or by e-mail to nstic@nist.gov.

V. Application 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 - 60 points, weights for sub-criteria i. through iv. listed below).** Reviewers will evaluate the extent to which the proposed operational pilot meets the following guiding principles as supported by the description of the operational pilot, including its architecture and data flows. The reviewers will also evaluate whether and how the proposed operational pilot maps critical elements to the NSTIC derived requirements. (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 (0-45 points; each sub-criterion is worth 15 points)** – The envisioned Identity Ecosystem will mitigate privacy and civil liberties risks engendered by an increased capability for identification, tracking, and personal data aggregation in stronger, federated identity solutions.

         Reviewers will evaluate how privacy and civil liberties will be protected, how that protection will be implemented on a technical and/or policy level, and the balance between selected technical and policy controls based on their effectiveness to mitigate identified risks. Specifically, reviewers will evaluate the following:

         (1) **Privacy-Enhancing Capabilities (0 - 15 points):** How the solution exhibits privacy-enhancing capabilities in support of the privacy goals of the pilot, including:

            - The manner in which it enables individuals and other pilot participants to have reliable assumptions about what personal information is being processed by project participants (the project lead, contractors, subawardees and other collaborators) and the rationale for such processing[3];
            - The manageability of personal information, including the capability for alteration, deletion and selective disclosure; and

[3] Processing means all actions of the system(s) that operate on personal information, including collection, generation or transformation, use, retention, disclosure or transmission and disposal.

- The manner in which personal information or events can be processed without association or the potential for association with individuals beyond operational requirements[4].

(2) Identity Assurance (0 - 15 points): How the solution provides assurance, as appropriate, for:

- Accuracy standards for personal information used in identity assurance, authentication or authorization components of the pilot;
- Compliance, audit, and verification that personal information is being processed in accordance with pilot policies; and
- Effective redress mechanisms for individuals experiencing adverse effects from the processing of their personal information.

(3) Mitigation of Privacy and Civil Liberties Risks (0 - 15 points): The strength and potential effectiveness of the mechanisms proposed for mitigating identified privacy and civil liberties risks consistent with subsections (1) and (2) above, including:

- The controls implemented to mitigate privacy and civil liberties risks, including whether policy or technical measures are used for each risk, and why any, in any given case, (i) a policy measure is more appropriate than a technical measure and (ii) the project participant implementing the control is more appropriate than another project participant;

- The quality of identified metrics for evaluating the privacy controls; and

- Any mechanisms or design choices used to enable individuals to have control over or manage their personal information.[5]

ii. Secure and resilient (0 - 5 points) – Reviewers will evaluate the appropriateness, quality, and completeness of how the proposed operational pilot provides security and resiliency. Security ensures the confidentiality,

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

[5] Control points for individuals should not be used to mitigate privacy risks created by architecture design or to mitigate risks that individuals could not be reasonably expected to be able to assess.

integrity and availability of identity solutions, information stores, 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.

Reviewers will evaluate how effectively the proposed solution:

- Embraces security mechanisms that provide material security advances over the password-based regime dominant in the marketplace today;
- Provides secure and reliable methods of electronic authentication; and
- Demonstrates the integration of all major aspects of the project.

iii. Interoperable (0 - 5 points)– Reviewers will evaluate the extent to which the proposed operational pilot enables interoperability. 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 evaluate how well the proposed solution fosters the reduction and elimination of policy and technology silos and adheres to open standards. Proprietary solutions that limit interoperability will be considered less competitive.

Reviewers will evaluate how effectively the proposed solution:

- Leverages existing standards and/or demonstrates the need for new standards;
- Materially advances the development and adoption of new standards;
- May be used across multiple sectors and RPs; and
- Allows for individual credentials to be simply and securely portable between RPs with appropriate notifications to individuals.

iv. Cost-effective and easy to use (0 - 5 points) – Reviewers will evaluate the extent to which the pilot implementation will be simple to understand, intuitive, easy to use, and enabled by technology that requires minimal user training.

Reviewers will evaluate how effectively the proposed solution:

- Overcomes any significant usability challenges;
- Provides for reasonable cost per user and how these costs affect the potential growth of the Identity Ecosystem in accordance with NSTIC's four guiding principles (*see* Section I of this FFO);
- Lowers barriers for user acceptance and can be easily incorporated into current user activities;
- Provides for the reuse of credentials by end-users across multiple services, relying parties and sectors; and

- Establishes service level agreements with easy to understand opt-in choices for the consumer to use a service.

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

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

Reviewers will evaluate the following:

- The completeness of all participants' plans during the project;
- How realistic and achievable are the measurable milestones set by the applicant, including metrics encompassing all work on the project including all participants;
- The quality of the project leadership's plans to manage the project including overseeing the work of all project participants including sub-recipients, contractors, etc. to ensure realization of project goals and objectives; and
- Alignment of the project plan to producing results consistent with the NSTIC guiding principles

c. Contribution to Identity Ecosystem (0 - 10 points).

Reviewers will evaluate the following:

- The uniqueness of the contribution to the NSTIC vision**;**
- The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into production expanding beyond initial pilot users; and
- The quality, comprehensives and extent of the contribution of the project to the broader development of the Identity Ecosystem Framework as described in the NSTIC strategy

d. Resource Availability (0 - 10 points).

Reviewers will evaluate the following:

- The appropriateness of the qualifications of the key personnel;
- The sufficiency of the time commitments of the key personnel;
- The appropriateness of the overall project resources to the project's scope and specific activities; and

- The cost-effectiveness of the project.

2. **Selection Factors.** The Selecting Official, who is the Chief Cybersecurity Advisor for NIST or her designee, 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 privacy guiding principle from being fully realized within the Identity Ecosystem.
   d. Diversity of technical approaches to proving a foundation for the implementation of the privacy guiding principle in federated identity credentials.
   e. Complementarity to other efforts, including both pilots and products of the IDESG, addressing the implementation of the Identity Ecosystem.

3. **Review and Selection Process**

a. Initial Administrative Review of Applications. 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. Applications determined to be ineligible, incomplete, and/or non-responsive may be eliminated from further review.

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

(1) Evaluation and Review. At least three independent, objective reviewers, who are Federal employees, knowledgeable in the subject matter of this FFO and its objectives will evaluate each application based on the evaluation criteria (*see* Section V.1. of this FFO). While every application will have at least three reviews, applications may have differing numbers of reviews if specialized expertise is needed to evaluate the application. These reviews, including comments and numerical scores, 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 use the reviewers' numeric scores to provide an initial ranking of the applications .Board members will then set a minimum numeric score for competitive applications based on the availability of funds and the quality of the applications.

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. If deemed necessary, each competitive applicant will be invited to participate in a web conference, or in person meeting with the Evaluation Board. Applicants may also be asked to provide updated commitment letters from potential project participants at that time. Each Evaluation Board member will assign each application a numeric score by applying the evaluation criteria to each competitive application, taking into account the additional information from written responses to questions and/or in person meeting or webinar.

(2) Ranking and Selection. Based on the Evaluation Board members' final numeric scores, a final rank order of the competitive applications 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 some, all, or none of the application(s) or part(s) of any particular application. The final approval of selected applications and issuance of awards will be by the NIST Grants Officer. The award decisions of the Grants Officer are final.

c. Federal Awarding Agency Review of Risk Posed by Applicants. After applications are proposed for funding by the selecting official, the NIST Grants Management Division performs administrative reviews. These may include reviews of the financial stability of an applicant, quality of the applicant's management systems, history of performance, and the applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-Federal entities. Upon review of these factors, if appropriate, special conditions that correspond to the degree of risk may be applied to an award.

4. Anticipated Announcement and Award Date. Review of Full Applications, selection of successful applicants, and award processing is expected to be completed in September 2015. The earliest anticipated start date for awards under this FFO is expected to be September 2015.

5. Additional Information

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

b. 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.

c. 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. Federal Award Administration Information

1. Federal 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://go.usa.gov/SNMR.

2. Administrative and National Policy Requirements

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

b. Department of Commerce Financial Assistance Standard Terms and Conditions. The Department of Commerce Financial Assistance Standard Terms and Conditions (December 26, 2014) will apply to this award and are accessible at: http://go.usa.gov/hKbj.

c. Pre-Award Notification Requirements. The Department of Commerce Pre-Award Notification Requirements for Grants and Cooperative Agreements, 79 FR 78390 (December 30, 2014), are applicable to this FFO and are available at http://go.usa.gov/hKkR.

d. 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.

e. Collaborations with NIST Employees. All applications should include a description of any work proposed to be performed by an entity other than the applicant, and the cost of such work should ordinarily be included in the budget.

If an applicant proposes collaboration with NIST, the statement of work should include a statement of this intention, a description of the collaboration, and prominently identify the NIST employee(s) involved, if known. Any collaboration by a NIST employee must be approved by appropriate NIST management and is at the sole discretion of NIST. Prior to beginning the merit review process, NIST will verify the approval of the proposed collaboration. Any unapproved collaboration will be stricken from the application prior to the merit review.

f. Use of NIST Intellectual Property. If the applicant anticipates using any NIST-owned intellectual property to carry out the work proposed, the applicant should identify such intellectual property. This information will be used to ensure that no NIST employee involved in the development of the intellectual property will participate in the review process for that competition. In addition, if the applicant intends to use NIST-owned intellectual property, the applicant must comply with all statutes and regulations governing the licensing of Federal government patents and inventions, described in 35 U.S.C. §§ 200-212, 37 C.F.R. Part 401, 2 C.F.R. §200.315, and in Section D.03 of the DoC Financial Assistance Terms and Conditions dated December 26, 2014, found at http://go.usa.gov/hKbj. Questions about these requirements may be directed to Chief Counsel for NIST, (301) 975-2803, nistcounsel@nist.gov.

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

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

g. Research Activities Involving Human Subjects, Human Tissue, Data or Recordings Involving Human Subjects Including Software Testing. Any application that includes research activities involving human subjects, human tissue/cells, or data or recordings involving human subjects, including software testing, must satisfy 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. Research activities involving human subjects who fall within

the classes of subjects found in 45 C.F.R. Part 46, Subparts B, C and D must satisfy the requirements of the applicable subpart. 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 activities include research involving 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 an application includes research activities which involve human subjects, the applicant 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 for those activities 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 research activities involving human subjects. 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. Both domestic and foreign organizations performing non-exempt research activities involving human subjects will be required to have protocols approved by a cognizant, active IRB currently registered with the Office for Human Research Protections (OHRP) within the DHHS that is linked to the engaged organizations. All engaged organizations must possess a currently valid Federalwide Assurance (FWA) on file from OHRP. Information regarding how to apply for an FWA and register an IRB with OHRP can be found at http://www.hhs.gov/ohrp/assurances/index.html. NIST relies only on OHRP-issued FWAs and IRB Registrations for both domestic and foreign organizations for NIST supported research involving human subjects. NIST will not issue its own FWAs or IRB Registrations for domestic or foreign organizations.

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, and which institutions are expected to be engaged in the research activities.

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 information may be requested for that activity/task:

(1) 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 in the Common Rule. *See* 15 C.F.R. § 27.102 Definitions.
(2) If the applicant participant(s) uses a cognizant IRB that provides a determination that the activity/task is not research, a copy of that determination 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/determination documentation will be required by NIST.

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

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 To what does this policy apply?):

(1) 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.
(2) A copy of the protocol for the research to be conducted; and/or the biological materials or data from human subjects to be collected/provided, not pre-existing samples (*i.e.,* will proposed research collect only information without personal identifiable information, will biological materials or data be de-identified and when and by whom was the de-identification performed, how were the materials or data originally collected).
(3) 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.
(4) Any additional clarifying documentation that NIST may request during the review process in order to make a determination that the activity/task or use of biological materials or data from human subjects is exempt under the Common Rule (*see* 15 C.F.R. § 27.101 To what does this policy apply?).

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 registered with OHRP, the following information may be requested during the review process:

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

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.)

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

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

For more information regarding research projects involving human subjects, contact Jason Boehm, Director, NIST Program Coordination Office (e-mail: jason.boehm@nist.gov; phone: (301) 975-8678.

3. Reporting

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

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

(2) Performance (Technical) Reports. Each award recipient will be required to submit a technical progress report to the NIST Grants Officer and the NSTIC NPO Federal Program Officer on a quarterly basis for the periods ending March 31, June 30, September 30, and December 31 of each year. Reports will be due within 30 days after the end of the reporting period. A final technical progress report shall be submitted within 90 days after the expiration date of the award. Technical progress reports shall contain information as prescribed in 2 C.F.R. § 200.328.

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

(4) NSTIC NPO Program Management. Each award recipient is expected to participate in a kickoff meeting within the first thirty days of award and detailed design reviews within sixty days of award and an update of the design review within six months of award. These design reviews will include the details of the

technical design of the solution overview such as the privacy enhancing technology deployed, architecture, data flows (including flows of personal information), interfaces, use cases risks and plans for mitigating those risks, etc., as well as demonstrate how the pilot meets the NSTIC guiding principles. In addition, the NSTIC NPO can require additional specialized reviews against any of the NSTIC guiding principles or specific aspects of the solution, as needed.

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

b. Audit Requirements. A non-Federal entity (as defined in 2 C.F.R. § 200.69) that expends $750,000 or more in Federal award funds during the non-federal entity's fiscal year is required to conduct a single or program-specific audit in accordance with the requirements set forth in 2 C.F.R. part 200, Subpart F. In addition, pursuant to Section F. of the Department of Commerce Financial Assistance Standard Terms and Conditions (December 26, 2014), non-Federal entities that are not subject to Subpart F of 2 C.F.R. Part 200 (e.g., for-profit entities) and that expend $750,000 or more in Department of Commerce award during their fiscal year must have an audit conducted for that year in accordance with Subpart F of 2 C.F.R. Part 200, unless otherwise specified in the terms and conditions of an award, Applicants are reminded that NIST, the DoC Office of Inspector General or another authorized Federal agency may conduct an audit of an award at any time.

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

VII. Federal Awarding Agency Contact(s)

Questions should be directed to the following contact persons:

Subject Area	Point of Contact
Programmatic and Technical Questions	Barbara Cuthill Phone: (301) 975-3273 E-mail: barbara.cuthill@nist.gov
Technical Assistance with Grants.gov Submissions	Christopher Hunton Phone: (301) 975-5718 Fax: (301) 975-6319 E-mail: christopher.hunton@nist.gov Or www.grants.gov Phone: (800) 518-4726 E-mail: support@grants.gov
Grant Rules and Regulations	Dean Iwasaki Phone: (301) 975-8449 Fax: (301) 975-6319 E-mail: dean.iwasaki@nist.gov
Use of NIST Intellectual Property	Chief Counsel for NIST Phone: (301) 975-2803 E-mail: nistcounsel@nist.gov
Use of Human Research Subjects	Jason Boehm Phone: (301) 975-8678 E-mail: jason.boehm@nist.gov

VIII. Other Information

Public Meetings (Webinar): NIST will hold a webinar 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 webinar or at any time before submitting the application to NIST. Also, NIST/NSTIC Program Office staff will not critique or provide feedback on project ideas while they are being developed by an applicant. Attendance at the Webinar is **not required. Information on the Webinar is available at www.nist.gov/nstic.**