March 31, 2016

ANNOUNCEMENT OF FEDERAL FUNDING OPPORTUNITY (FFO)
National Strategy for Trusted Identities in Cyberspace (NSTIC)
Federated Identity in Healthcare Pilot 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) Federated Identity in Healthcare Pilot Program

- **Announcement Type:** Initial

- **Funding Opportunity Number:** 2016-NIST-NSTIC-02

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

- **Dates:** Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, Wednesday, June 1, 2016. Applications received after this deadline will not be reviewed or considered. **Applicants should be aware, and factor in their application submission planning, that the Grants.gov system is expected to be closed for routine maintenance at these times: from 12:01 a.m. Eastern Time, Saturday, April 16, 2016 until Monday, April 18, 2016 at 6:00 a.m. Eastern Time; and again from 12:01 a.m. Eastern Time, Saturday, May 21, 2016 until Monday, May 23, 2016 at 6:00 a.m. Eastern Time. Applications cannot be submitted when Grants.gov is closed**. NIST expects to complete its review, selection of successful applicants, and award processing by September 2016. NIST expects the earliest anticipated start date for awards under this FFO to be October 1, 2016.

  Applicants are strongly urged to read Section IV.2.b., Attachment of Required Application Documents, found on page 15 of this FFO, with great attention. Applicants should carefully follow the instructions and recommendations regarding attachments and using Grants.gov's Download Submitted Applications feature to check that all required attachments were contained in their submission. Applications submitted without the required documents will not pass the Initial Administrative Review, described in Section V.3.a. of this FFO.

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

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

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

- **Funding Opportunity Description:** NIST is soliciting applications from eligible applicants to demonstrate the usage of federated online identity solutions for patients and providers across multiple healthcare providers (e.g., provider groups, regional healthcare systems, hospital systems).

- **Anticipated Amounts:** NIST anticipates funding one award in the range of $750,000 to $1,000,000 for eighteen months.

- **Funding Instrument:** Cooperative agreement.

- **Who Is Eligible:** All applicants must meet all of the following requirements:

    - Applicants must be hospitals or healthcare systems consisting of multiple hospitals, ambulatory sites, clinics or similar healthcare facilities.
    - Applicants may be for-profit, not-for-profit or governmental (other than Federal government) entities located in the United States or its territories.
    - Applicants must partner with at least one other healthcare organization in their locality/region. The partner organization should have anticipated overlap with the applicant organization of patients, physicians and other clinical staff (such as a physician practice group(s), clinic(s) and hospital(s)).
    - The partner organization must be organizationally independent of the applicant and maintain a separate health information system from the applicant. Health information systems refer to any system that captures, stores, manages or transmits information related to the health of individuals or the activities of organizations that work within the health sector.

    NIST will not assist in matching organizations. Federal agencies (including facilities and components of the Veteran's Integrated Service Network of the Veteran's Health Administration) may participate in projects but may not receive NIST funding.

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

- **Public Meetings (Applicants' Conference):** NIST will hold a webinar (Applicants' Conference) to provide general information regarding the NSTIC, offer general guidance on preparing applications, and answer questions. The Office of the National Health Coordinator at the Department of Health and Human Services (ONC) may provide additional seminars to offer general information on the use of federated identity credentials in the healthcare sector. Proprietary technical discussions about specific project ideas with NIST or ONC staff are not permitted at any time before submitting an application to NIST. Therefore, applicants should not raise proprietary issues at the Applicants' Conference or any additional seminars related to this competition. Also, NIST and ONC staff will not critique or provide feedback on specific project ideas while they are being developed by an applicant. However, questions about the National Strategy for Trusted Identities in Cyberspace (NSTIC) Federated Identity in Healthcare Pilot Program eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application at the Applicants' Conference and by email to nstic@nist.gov. Attendance at the Applicants' Conference or any ONC sponsored events is not required. Information on the Applicants' Conference and any related ONC sponsored events is available at http://www.nist.gov/nstic/funding-opportunities.html.

Table of Contents

FULL ANNOUNCEMENT TEXT

I. Program Description

The statutory authority for the National Strategy for Trusted Identities in Cyberspace (NSTIC or Strategy) Federated Identity in Healthcare Pilot Program is 15 U.S.C. §§ 272(b)(1), (b)(4), (c)(12), and (c)(14).

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

The Strategy envisions a user-centric Identity Ecosystem, defined as "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices."[1]

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

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

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

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

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

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

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

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

NIST Funded Projects Advancing the NSTIC Strategy

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

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

In Section 3001(c)(3)(A) of the Public Health Service Act (PHSA), as added by Section 13101 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII of Division A of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5), Congress directed the Office of the National Coordinator for Health Information Technology (ONC) at the U.S. Department of Health and Human Services to work with other federal agencies, including NIST, to update the Federal Health IT Strategic Plan to include specific objectives, including the utilization of electronic health records (EHRs) and ensuring privacy and security protections for such records.

In July 2010, ONC published a final rule, codified at 45 CFR Part 170, that established certification criteria for EHRs. The final rule notably included the requirement that Certified EHR Technology have the capability to verify that a person or entity seeking access to electronic health information is the individual claimed and is authorized to access such information (45 CFR 170.302(t)).

This project will consist of one cooperative agreement award from NIST and will include continued collaboration with the ONC. While the ONC will not provide grant funding, the ONC anticipates offering technical assistance to grantee(s), including using a contractor with subject matter expertise in identity management solutions to coordinate and support the pilot(s).

Federated Identity in Healthcare Pilot Program: Digitally Delivering Trustworthy Constituent Services

The purpose of the NSTIC Federated Identity in Healthcare Pilot Program is to demonstrate the usage of federated online identity solutions for patients and providers across at least two healthcare providers and provide a basis for documenting best practices in this area. The proposed identity solutions must embrace and advance the NSTIC vision of an Identity Ecosystem.

Currently, patients and providers need to obtain new identity credentials to access health information at different organizations. Technologies exist to streamline authentication to web portals today but mostly exist to service one organization only. This funding opportunity will support a pilot project involving multiple healthcare organizations to enable patients and providers to use a single credential that can be trusted to allow access to health medical records.

The goal for this project is for hospital systems to work with other regional health systems and provider groups to operationalize the acceptance of federated identity and operate the pilot for at least six months. The use cases for this pilot would involve a federated credential solution that allows patients and health care providers to use the same credential with at least two healthcare organizations.

Specifically, the applicant's project must:

1. Pilot a federated credential solution in which at least two hospitals or regional healthcare systems accept a federated, verified identity that leverages multi-factor authentication and an effective identity proofing process.
2. Enable online access to at least two organizationally separate healthcare organizations.
3. Demonstrate that the federated credential solution aligns with the Identity Ecosystem Framework Requirements.
4. Allow for interoperability with other identity federations in the healthcare sector and, where possible, other sectors.
5. Include collecting metrics and other information about the implementation of the federated credential solution that can contribute to a best practices guidance document.

ONC will be participating in the review of applications and may provide technical support regarding implementation and operation of pilot. A successful project will

generate the data necessary for ONC, NIST, and the project participants to jointly publish a document on best practices for identity management in the healthcare sector with working examples and other guidelines and lessons learned for use in the healthcare and other sectors. Additionally, a successful project will help catalyze the adoption of federated identity credentials in the healthcare sector.

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

II. Federal Award Information

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

2. **Funding Availability.** NIST anticipates funding one award in the range of $750,000 to $1,000,000 for eighteen months.

III. Eligibility Information

1. Who Is Eligible: All applicants must meet all of the following requirements:

- Applicants must be hospitals or healthcare system consisting of multiple hospitals, ambulatory sites, clinics or similar healthcare facilities.
- Applicants may be for-profit, not-for-profit or governmental (other than Federal government) entities located in the United States or its territories.
- Applicants must partner with at least one other healthcare organization in their locality/region. The partner organization should have anticipated overlap with the applicant organization of patients, physicians and other clinical staff (such as a physician practice group(s), clinic(s) and hospital(s)).
- The partner organization must be organizationally independent of the applicant and maintain a separate health information system from the applicant. Health information systems refer to any system that captures, stores, manages or transmits information related to the health of individuals or the activities of organizations that work within the health sector.

NIST will not assist in matching organizations. Federal agencies (including facilities and components of the Veteran's Integrated Service Network of the Veteran's Health Administration) 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 under Funding Opportunity Number 2016-NIST-NSTIC-02.

2. Content and Format of Application Submission

a. Required Forms and Document

The Application must contain the following:

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

- SF-424, Item 12, should list the FFO number 2016-NIST-NSTIC-02.
- SF-424, Item 18, should list the total Federal budget amount requested for the entire project.
- For SF-424, Item 21, the list of certifications and assurances is contained in the SF-424B.

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

The Grant Program Function or Activity on Line 1 under Column (a) should be entered as "Arrangements for Interdisciplinary Research Infrastructure". The Catalog of Federal Domestic Assistance Number on Line 1 under Column (b) should be entered as "11.619".

These sections of the SF-424A should reflect funds for the whole 18-month term of the award: Section A; Section B; Section C; and Section D.

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

(4) CD-511, Certification Regarding Lobbying. Enter "2016-NIST-NSTIC-02" in the Award Number field. Enter the title of the application used in field 15 of the SF-424, or an abbreviation of that title, in the Project Name field.

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

(6) Technical Proposal. The Technical Proposal is a document of no more than 25 pages responsive to the program description (*see* Section I. of this FFO) and the evaluation criteria (*see* Section V.1. of this FFO). The Technical Proposal should contain the following information:

(a) **Executive Summary.** An executive summary of the proposed project, including listing the proposed project participants, the scope of the proposed use case, the proposed source for the federated identity solution and the timeline for the planned metrics collection effort.

(b) **Problem Statement and Use Cases.** A problem statement that discusses the specific use cases (e.g., provider and patient) to be demonstrated including the specific separate organizations participating in each use case and the size of the populations at each organization involved. Any special characteristics of the populations should be noted.

(c) **Federated Identity Solution.** A description of the identity federation solution chosen and the technical architecture to be implemented for the proposed effort. This solution should leverage readily available commercial identity credentials and products to the extent possible. In addition, this solution should support pseudonymous identities with verified attributes based on effective identity proofing as appropriate to the use cases involved. This section should include information on all the components of the solution, how these components interconnect, and what information is exchanged among the components. An architecture diagram and data flow diagrams including data flows among project participants may be used to present this information and will not be counted within the page limit. The applicant should provide information on the steps that need to be taken to initiate the project, complete the project, and evaluate the results.

The solution should be compliant with all applicable laws and regulations, including:

- 45 C.F.R. § 170.315(d)(1) [2015 Edition health IT certification criteria];
- 45 C.F.R. § 164.312(a)(1) [Technical safeguards: Standard Access control]; and

- 45 C.F.R. § 164.312(d) [Technical safeguards, Standard: Person or entity authentication], which states “implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed”.

The solution description, including any architecture and data flow diagrams, should make clear how the solution mitigates privacy and civil liberties risks arising from the capability for greater identification, tracking or linkability of transactions, and personal data aggregation. Privacy and civil liberties protections may be enforced by either (or both) technical and policy means; however, technical means for mitigating privacy risks are preferable to policy mitigations. This section should explain how the technical and policy measures are applied in a risk-based approach to address privacy concerns - for example, NIST’s privacy risk model as documented in *Privacy Risk Management for Federal Information Systems,* NISTIR 8062 *(DRAFT)* (http://csrc.nist.gov/projects/privacy_engineering/documents.html).

This section should address the evaluation criteria V.1.a. through e. of this FFO.

(d) **Metrics Collection.** A description of the plans to collect metrics during at least a six-month period while the project is operational. The specific metrics to be collected should be presented. This section should address the *Project Impact* evaluation criterion (*see* Section V.1.f. of this FFO).

Collected metrics should include, at minimum, pre- and post-operational pilot. To this end, the applicant must determine the matrices and begin metrics collection process prior to the operational phase and continue collection through the end of the operational phase. Implementation plans for the pilots will be expected to include tasks that measure the pre- and post- results and include reports on collected metrics throughout the course of the project. Applicants should anticipate that tracking on the progress of the pilot will be made publicly available, including the baseline comparison of results from the pre and post operational phases (to determine if the intervention affected the outcome).

(e) **Statement of Work and Implementation Plan.** A complete statement of work covering all project participants that includes the following:

- Specific information about each organization that will be involved in the project and how the organizations will interact with one another (e.g., how one organization will use another’s federated identity credentials);
- Specific proposed tasks;

- Schedule of measurable events and realistic, measurable milestones for the overall project;
- Timeline for inclusion of each partner in the federated identity solution pilot;
- Timeline for metrics collection;
- Measurable performance objectives used to determine the success of the pilot along with the required metrics to indicate success; and
- The project leadership's plans to manage all project participants, including sub-recipients, contractors, etc., to ensure realization of project goals and objectives.

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

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

(f) **Qualifications.** A description of the qualifications, proposed roles, and level of planned effort of the project participants, including the proposed role of the project lead and of each subawardee, contractor, or other collaborator participating in the project. Include a discussion of the partners' past experience collaborating with each other, if applicable.

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

- At least one individual from each participant, with details of committed participation.
- 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 similar endeavors.
- At least one privacy engineer with specialized knowledge of both privacy technology and policy issues is required. This individual 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/or job skills. Qualifications for the privacy skillset could include certifications such as CIPT or CIPM and experience implementing privacy principles such as the Fair Information Practice Principles, identifying and mitigating privacy risks in the implementation of information technology systems. Qualifications for the technical skillset could include advanced degrees in computer science, information science, or computer engineering and experience with architectural design for information systems; data, systems, or software engineering; and related aspects of technical privacy implementations. If multiple individuals are used to meet this qualification, the applicant must include a description of how the multiple individuals will work together to compensate for the lack of the combined skillset in a single individual.

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

Resumes of all key personnel are required and are not included in the page count. Resumes should be a maximum of 2 pages each.

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

(7) Budget Narrative. The Budget Narrative should provide a detailed breakdown of each of the object class categories as reflected on the SF-424A. The budget justification should address all of the budget categories (personnel, fringe benefits, equipment, travel, supplies, other direct costs and indirect costs). The written justification should include the necessity and the basis for the cost. Proposed funding levels must be consistent with the project scope, and only allowable costs should be included in the budget. Information on cost allowability is available in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200 (http://go.usa.gov/SBYh), which apply to awards in this program. Information needed for each category is as follows:

(a) **Personnel** – At a minimum, the budget justification for all personnel should include the following: name, job title, commitment of effort on the proposed project in terms of average number of hours per week or percentage of time, salary rate, total direct charges on the proposed project, description of the role of the individual on the proposed project and the work to be performed. Applicants can include in the budget the time to participate in forums (such as committees of the IDESG) developing elements of the Identity Ecosystem Framework as envisioned in the Strategy. The cost of the time required to

prepare presentations to report on the progress of the project to the IDESG should also be included in this category.

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

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

(d) **Travel** – NIST will require that award recipients report on their projects twice a year to the Identity Ecosystem Steering Group (http://www.idecosystem.org/). Therefore, applicants should include travel costs for at least two meetings of the IDESG per year. 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 and number of people traveling; dates and/or duration; mode of transportation, lodging and subsistence rates; and description of how the travel is directly related to the proposed project. For travel that is yet to be determined, please provide best estimates based on prior experience. If a destination is not known, an approximate amount may be used with the assumptions given for the location of the meeting.

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

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

(g) **Other Direct Costs** – For costs that do not easily fit into the other cost categories, please list the cost, and the breakdown of the total costs by

quantity or unit of cost. Include the necessity of the cost for the completion of the proposed project. Only allowable costs can be charged to the award.

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

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

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

(a) **Letters of Commitment to participate**. The application must include letters of commitment from each healthcare organization participating in the project that describe its participation and the level of organizational commitment to the project. If the application identifies other third parties including contractors, subawardees, or other collaborators, who will participate in the proposed project, then the applicant must provide a letter from each currently known participant describing its participation. 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.h. of this FFO).

(b) **Additional Letters of Commitment or Interest,** optional. Letters of commitment and letters of interest may be provided from other parties who might become adopters of the solutions discussed in the proposed project after the pilot period.

(10) Resumes of Key Personnel including Privacy Experts. Resumes of all key personnel, note that the resumes are part of the material addressing *Resource Availability* evaluation criterion (*see* Section V.1.h. of this FFO).

(11) Data Management Plan. In accordance with the Office of Science and Technology Memorandum for the Heads of Executive Departments and

Agencies of February 22, 2013[2], *Increasing Access to the Results of Federally Funded Scientific Research*, and as implemented through NIST Policy 5700.00[3], *Managing Public Access to Results of Federally Funded Research,* and NIST Order 5701.00[4], *Managing Public Access to Results of Federally Funded Research*", applicants should include a Data Management Plan (DMP).

The DMP is a supplementary document of not more than two pages that must include, at a minimum, a summary of proposed activities that are expected to generate data, a summary of the types of data expected to be generated by the identified activities, a plan for storage and maintenance of the data expected to be generated by the identified activities, and a plan describing whether and how data generated by the identified activities will be reviewed and made available to the public. As long as the DMP meets these NIST requirements, it may take the form specified by the applicant's institution or some other entity (e.g., the National Science Foundation[5] or the National Institutes of Health[6]). Some organizations' templates are available on the Internet.[7]

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

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

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

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

b. Attachment of Required Documents

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

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

[2] https://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf
[3] http://www.nist.gov/open/upload/Final-P-5700.pdf
[4] http://www.nist.gov/open/upload/Final-O-5701_0.pdf
[5] http://www.nsf.gov/bfa/dias/policy/dmp.jsp
[6] http://grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm
[7] https://www.cic.net/projects/technology/shared-storage-services/data-management-plans

Applicants should carefully follow specific Grants.gov instructions at www.grants.gov to ensure the attachments will be accepted by the Grants.gov system. ***A receipt from Grants.gov indicates only that an application was transferred to a system. It does not provide details concerning whether all attachments (or how many attachments) transferred successfully.*** Applicants using Grants.gov will receive a series of e-mail messages over a period of up to two business days before learning whether a Federal agency's electronic system has received its application.

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

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

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

c. Application Format

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

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

(3) Font. Easy to read font (10-point minimum). Smaller type may be used in figures and tables but must be clearly legible.

(4) Page Limit. The Technical Proposal for Applications is limited to twenty-five (25) pages.

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

Page limit excludes: SF-424, Application for Federal Assistance; SF-424A, Budget Information – Non-Construction Programs; SF-424B, Assurances – Non-Construction Programs; SF-LLL, Disclosure of Lobbying Activities; CD-511, Certification Regarding Lobbying; Cover Page; Gantt Chart, WBS, or other planning document (if included); Architecture and data flow diagrams (if included); detailed analysis of the privacy risks of the solution (e.g., an

analysis against NIST's privacy risk model (see http://csrc.nist.gov/projects/privacy_engineering/documents.html); Budget Narrative; Indirect Cost Rate Agreement; Letters of Commitment or Interest; Resumes of Key Personnel; and Data Management Plan.

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

(6) Application language. English.

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

e. Pre-Applications. There are no pre-applications with this FFO.

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

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

4. Submission Dates and Times. Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, Wednesday, June 1, 2016. **Applicants should be aware, and factor in their application submission planning, that the Grants.gov system is expected to be closed for routine maintenance at these times: from 12:01 a.m. Eastern Time, Saturday, April 16, 2016 until Monday, April 18, 2016 at 6:00 a.m. Eastern Time; and from 12:01 a.m. Eastern Time, Saturday, May 21, 2016 until Monday, May 23, 2016 at 6:00 a.m. Eastern Time. Applications cannot be submitted when Grants.gov is closed.** Applications received after this deadline will not be reviewed or considered. NIST expects to

complete its review, selection of successful applicants, and award processing by September 2016. NIST expects the earliest anticipated start date for awards under this FFO to be October 1, 2016.

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

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

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

7. **Other Submission Requirements**

a. Applications must be submitted electronically.

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

(a) Applicants should carefully follow specific Grants.gov instructions to ensure that all attachments will be accepted by the Grants.gov system. A receipt from Grants.gov indicating an application is received does not provide information about whether attachments have been received. For further information or questions regarding applying electronically for the 2016-NIST-NSTIC-02 announcement, contact Christopher Hunton by phone at 301-975-5718 or by e-mail at grants@nist.gov.

(b) Applicants are strongly encouraged to start early and not wait until the approaching due date before logging on and reviewing the instructions for submitting an application through Grants.gov. The Grants.gov registration process must be completed before a new registrant can apply electronically. If all goes well, the registration process takes three to five business days. If problems are encountered, the registration process can take up to two weeks or more. Applicants must have a valid unique entity identifier number and must maintain a current registration in the Federal government's primary registrant database, the System for Award Management (https://www.sam.gov/), as

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

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

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

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

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

The application must be both received and validated by Grants.gov. The application is "received" when Grants.gov provides the applicant a confirmation of receipt and an application tracking number. If an applicant does not see this confirmation and tracking number, the application has not been received. After the application has been received, it must still be validated. During this process, it may be "validated" or "rejected with errors." To know whether the application was rejected with errors and the reasons why, the applicant must log in to Grants.gov, select "Applicants" from the top navigation, and select "Track my application" from the drop-down list. If the status is "rejected with errors," the applicant may still seek

to correct the errors and resubmit your application before the deadline. If the applicant does not correct the errors, the application will not be forwarded to NIST by Grants.gov.

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

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

V. Application Review Information

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

a. Privacy-Enhancing Capabilities (0 to 12 points): Reviewers will evaluate the completeness and effectiveness of the applicant's proposed solution to provide privacy-enhancing capabilities including:

- How the solution enables users to make reliable assumptions about the personal information being processed by project participants (the project lead, contractors, subawardees and other collaborators).
- How the solution enables user management of personal information, including the capability for alteration, deletion and selective disclosure. Such capabilities may include the mechanisms or design choices used to enable individuals to have control over or manage their personal information. When individuals cannot alter their personal information, for example some elements of a health record, or regulation or law requires disclosure, then this fact should be transparent to the user.
- How the solution processes events without association or the potential for association with individuals beyond operational requirements. For example, the solution should not track users searching for general healthcare information or healthcare provider information.
- How the solution implements controls for mitigating privacy and civil liberties risks, including whether policy or technical measures are used for each risk, and why 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.

b. Strength of Identity Proofing Approach (0 to 12 points): Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the

applicant's proposed approach to leverage identity credentials issued by a federated partner using a secure and reliable method of identity proofing.

c. **Strength of Authentication Approach (0 to 12 points):** Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's proposed approach to leverage identity credentials issued by a federated partner using a secure and reliable method of authentication.

d. **Supports Standards for Interoperability (0 to 12 points):** Reviewers will evaluate how well the proposed solution complies with or leverages widely adopted interoperability standards and specifications, as appropriate, such as:

- Fast Identity Online (FIDO) (https://fidoalliance.org/specifications/overview/)
- Security Assertion Markup Language (SAML) (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)
- OpenID Connect (http://openid.net/foundation/)
- Open Authentication Standard (OAuth) (http://oauth.net/2/)
- User-Managed Access (UMA) (https://docs.kantarainitiative.org/uma/rec-uma-core.html)
- Fast Healthcare Interoperability Resources (FHIR) (http://www.hl7.org/implement/standards/fhir/).

e. **Ease of Use (0 to 12 points):** Reviewers will evaluate how usable the proposed solution is for the full population of users (i.e., including marginalized or underrepresented groups) to easily access health records and online services securely.

f. **Project Impact (0 to 15 points).**

Reviewers will evaluate:

- The size and diversity of the organizations and populations involved in the federated identity credential pilot;
- The extent of the activities to be included in the pilot;
- The extent of the potential impact to the community and the regional healthcare delivery system**;**
- The extent the project establishes new services or offerings for patients and providers that are not in use today**;**
- The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into routine use expanding beyond initial users and the award period; and
- The quality and extent of the proposed metrics collection effort.

g. **Quality of Implementation Plan (0 to 15 points).**

Reviewers will evaluate the appropriateness, quality, completeness and effectiveness of the applicant's plans for pilot implementation.

Specifically, reviewers will evaluate the following:

- The completeness of all participants' plans an appropriate level of detail for the following areas:
  - Major task descriptions,
  - Schedule,
  - Quantified Objectives,
  - Milestones with measurable metrics,
  - Method of evaluating the metrics,
  - Risks,
  - Plans for stakeholder outreach, and
  - Integration with other efforts to ensure the solution meets needs;
- The quality of the project leadership's plans to manage the project including managing the work of all project participants including sub-recipients, contractor's, etc., to ensure realization of project goals and objectives;
- The appropriateness of the measurable milestones; and
- The timeline for including at least six months of metrics collection on the active pilot.

h. Resource Availability (0 to 10 points).

Reviewers will evaluate:

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

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

a. The availability of Federal funds;
b. Whether the project duplicates other projects funded by NIST, DoC, or by other Federal agencies; and
c. Diversity of the portfolio of NSTIC projects and alignment with NSTIC priorities.

3. Review and Selection Process

a. Initial Administrative Review. An initial review of timely received applications will be conducted to determine eligibility, completeness, and responsiveness to this FFO. Responsiveness to the FFO includes identification of at least two healthcare organizations participating in the pilot and at least a six-month timeline during the project for metrics collection. Applications determined to be ineligible, incomplete, and/or non-responsive may be eliminated from further review. However, NIST, in its sole discretion, may continue the review process for an application that is missing non-substantive information which may easily be rectified or cured at a later point in the evaluation process.

b. 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 will be forwarded to an Evaluation Board, a committee comprised of Federal employees knowledgeable in the subject matter of this FFO and its objectives.

The Evaluation Board will rank the applications using the average of the reviewers' numeric scores (*see* Section V.2. of this FFO). Board members will then consider the written evaluations against the selection criteria and set a numeric score threshold for competitive applications.

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

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

NIST reserves the right to negotiate the budget costs with the selected applicant. Negotiations may include requesting that the applicant remove certain costs. Additionally, NIST may request that the applicant modify objectives or work plans

and provide supplemental information required by the agency prior to award. NIST also reserves the right to reject an application where information is uncovered that raises a reasonable doubt as to the responsibility of the applicant. NIST may select some, all, or none of the applications, or part(s) of any particular application. NIST may request that fundable applicants consider working together in a combined project if this approach might effectively advance the program mission. The final approval of selected applications and issuance of awards will be by the NIST Grants Officer. The award decisions of the Grants Officer are final.

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

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

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

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 years for record keeping purposes. After three 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 package from the NIST Grants Officer. The award cover page, i.e., CD-450, Financial Assistance Award is available at http://go.usa.gov/SNMR.

2. **Administrative and National Policy Requirements**

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

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

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

d. **Collaborations with NIST Employees.** No NIST employees may be named as collaborators on projects for this FFO.

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

Any use of NIST-owned intellectual property by 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.

f. Research Activities Involving Human Subjects, Human Tissue, Data or Recordings Involving Human Subjects Including Software Testing. Any application that includes research activities involving human subjects, human tissue/cells, or data or recordings from or about human subjects, must satisfy the requirements of the Common Rule for the Protection of Human Subjects ("Common Rule"), codified for the Department of Commerce at 15 C.F.R. Part 27. Research activities involving human subjects who fall within one or more of the classes of vulnerable subjects found in 45 C.F.R. Part 46, Subparts B, C and D must satisfy the requirements of the applicable subpart(s). In addition, any such application that includes research activities on these subjects must be in compliance with all applicable statutory requirements imposed upon the Department of Health and Human Services (DHHS) and other Federal agencies, all regulations, policies and guidance adopted by DHHS, the Food and Drug Administration, and other Federal agencies on these topics, and all Executive Orders and Presidential statements of policy on applicable topics. (Regulatory Resources: http://www.hhs.gov/ohrp/humansubjects/index.html which includes links to FDA regulations, but may not include all applicable regulations and policies).

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

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

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

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

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

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

See 15 C.F.R. § 27.102 Definitions.

1) **Requirement for Federalwide Assurance.** If the application is accepted for [or awarded] funding, organizations that have an IRB are required to follow the procedures of their organization for approval of exempt and non-exempt research activities that involve human subjects. Both domestic and foreign organizations performing non-exempt research activities involving human subjects will be required to have protocols approved by a cognizant, active IRB currently registered with the Office for Human Research Protections (OHRP) within the DHHS that is linked to the engaged organizations. All engaged organizations must possess a currently valid Federalwide Assurance (FWA) on file from OHRP. Information regarding how to apply for an FWA and register an IRB with OHRP can be found at http://www.hhs.gov/ohrp/assurances/index.html. NIST relies only on OHRP-issued FWAs and IRB Registrations for both domestic and foreign organizations for NIST supported research involving human subjects. NIST will not issue its own FWAs or IRB Registrations for domestic or foreign organizations.

2) **Administrative Review.** NIST reserves the right to make an independent determination of whether an applicant's activities include research involving human subjects. NIST will conduct an independent administrative review of all applications accepted for funding that include research involving human subjects that were approved by a non-NIST Institutional Review Board (IRB). Research may not start until the NIST Human Subjects Protection Office (HSPO) issues institutional review approval for final action by the NIST Grants

Officer. (15 C.F.R. § 27.112 Review by Institution.) If NIST determines that an application includes research activities which involve human subjects, the applicant will be required to provide additional information for review and approval. The documents required for funded proposals are listed in each section below. Most such documents will need to be produced during the proposal review process; however, the Grants Officer may allow final versions of certain required documents to be produced at an appropriate designated time post-award. If an award is issued, no research activities involving human subjects shall be initiated or costs incurred for those activities under the award until the NIST Grants Officer issues written approval. Retroactive approvals are not permitted.

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

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

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

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

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

(1) The name(s) of the institution(s) where the exempt research will be conducted.
(2) The name(s) of the institution(s) providing the biological materials or data from human subjects will be provided.
(3) A copy of the protocol for the research to be conducted; and/or the biological materials or data from human subjects to be collected/provided, not pre-existing samples (*i.e.,* will proposed research collect only information without personal identifiable information, will biological materials or data be de-identified and when and by whom was the de-identification performed, how were the materials or data originally collected).
(4) For pre-existing biological materials or data from human subjects, provide copies of the consent forms used for collection and a description of how the materials or data were originally collected and stripped of personal identifiers. If copies of consent forms are not available, explain.
(5) Any additional clarifying documentation that NIST may deem necessary in order to make a determination whether the activity/task or use of biological materials or data from human subjects is exempt under the Common Rule.

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

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

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

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

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

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

3. Reporting

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

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

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

(3) 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.

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

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

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

4. Award Management and Public Engagement

a. **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 should be provided at these presentations.

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

c. **Program Communication.** All pilot projects awarded under this program are expected to publish interim reports on the publicly releasable lessons learned from their projects to benefit similar efforts**.**

VII. Federal Awarding Agency Contacts

Questions should be directed to the following contact persons:

Subject Area	Point of Contact
Programmatic and Technical Questions	Barbara Cuthill Phone: 301-975-3273 E-mail: nstic@nist.gov
Technical Assistance with Grants.gov Submissions	Christopher Hunton Phone: 301-975-5718 Fax: (301) 975-8884 E-mail: grants@nist.gov Or Grants.gov Phone: (800) 518-4726 E-mail: support@grants.gov
Grant Rules and Regulations	Dean Iwasaki Phone: 301-975-8449 Fax: (301) 975-8884 E-mail: dean.iwasaki@nist.gov

VIII. Other Information

Public Meetings (Applicants' Conference): NIST will hold a webinar (Applicants' Conference) to provide general information regarding the NSTIC, to offer general guidance on preparing applications, and to answer questions. The Office of the National Health Coordinator at the Department of Health and Human Services (ONC) may provide additional seminars to offer general information on the use of federated identity credentials in the healthcare sector. Proprietary technical discussions about specific project ideas with NIST or ONC staff are not permitted at any time before submitting an application to NIST. Therefore, applicants should not expect to have proprietary issues addressed at the Applicants' Conference or any additional seminars on this topic. Also, NIST and ONC staff will not critique or provide feedback on specific project ideas while they are being developed by an applicant. However, questions about the National Strategy for Trusted Identities in Cyberspace (NSTIC) Federated Identity in Healthcare Pilot Program eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application at the Applicants' Conference and by email to nstic@nist.gov. Attendance at the Applicants' Conference or any ONC sponsored events is not required. Information on the Applicants' Conference and any related ONC sponsored events is available at http://www.nist.gov/nstic/funding-opportunities.html.