NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

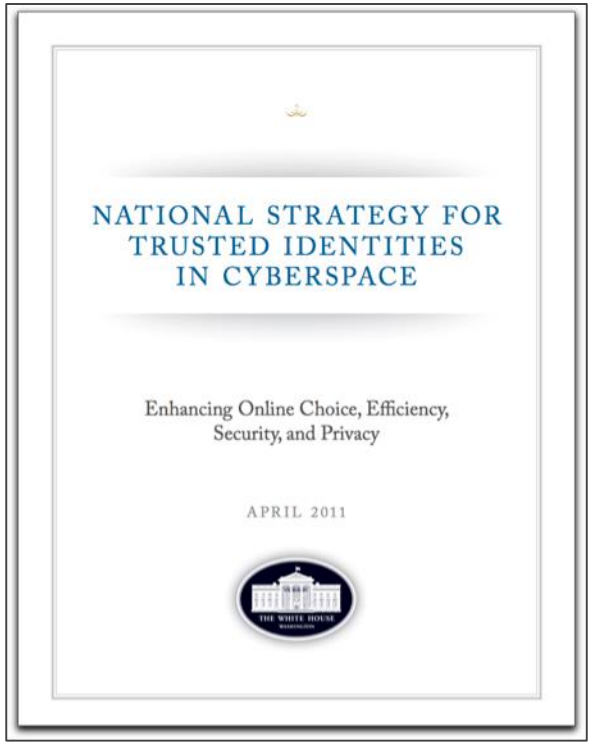
APPLICANTS WEBINAR

April 18, 2016

NSTIC OVERVIEW AND STATUS UPDATE

MICHAEL GARCIA
NSTIC ACTING DIRECTOR

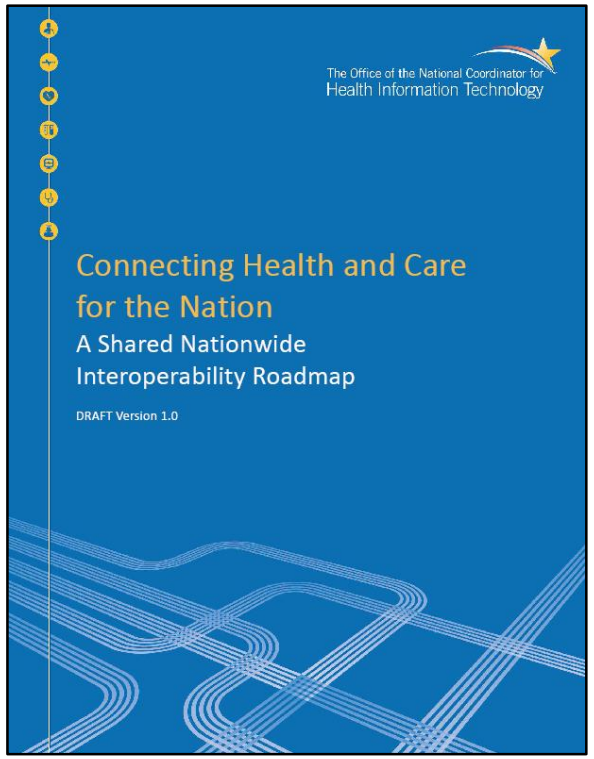
NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE



NSTIC vision

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.

IN PARTNERSHIP WITH ONC



A Shared Nationwide Interoperability Roadmap

The Office of the National Coordinator for Health Information Technology (ONC) is committed to achieving an interoperable health IT ecosystem that makes the right data available to the right people at the right time across products and organizations in a way that can be relied upon and meaningfully used by recipients.

IT’S 2011.

Most American adults (79%) use the Internet.
The average user needs 10 different passwords daily.
It’s a year of unprecedented breaches.
It’s the year Google releases two-factor authentication.

The U.S. government releases an ambitious strategy to improve digital identity and online interactions.

THE GOAL

Enhance online choice, efficiency, security, and privacy by fostering a marketplace of identity solutions

privacy enhancing & voluntary

secure & resilient

interoperable

cost effective & easy-to-use

THE MODEL: PART 1

convene the private sector

IDESG: independent 501(c)(3); ~300 members;
IDEF publicly released October 2015

---

catalyze a marketplace

18 pilots: 150+ partners; 3.8 million impacted;
11 industries; 10 MFA solutions

---

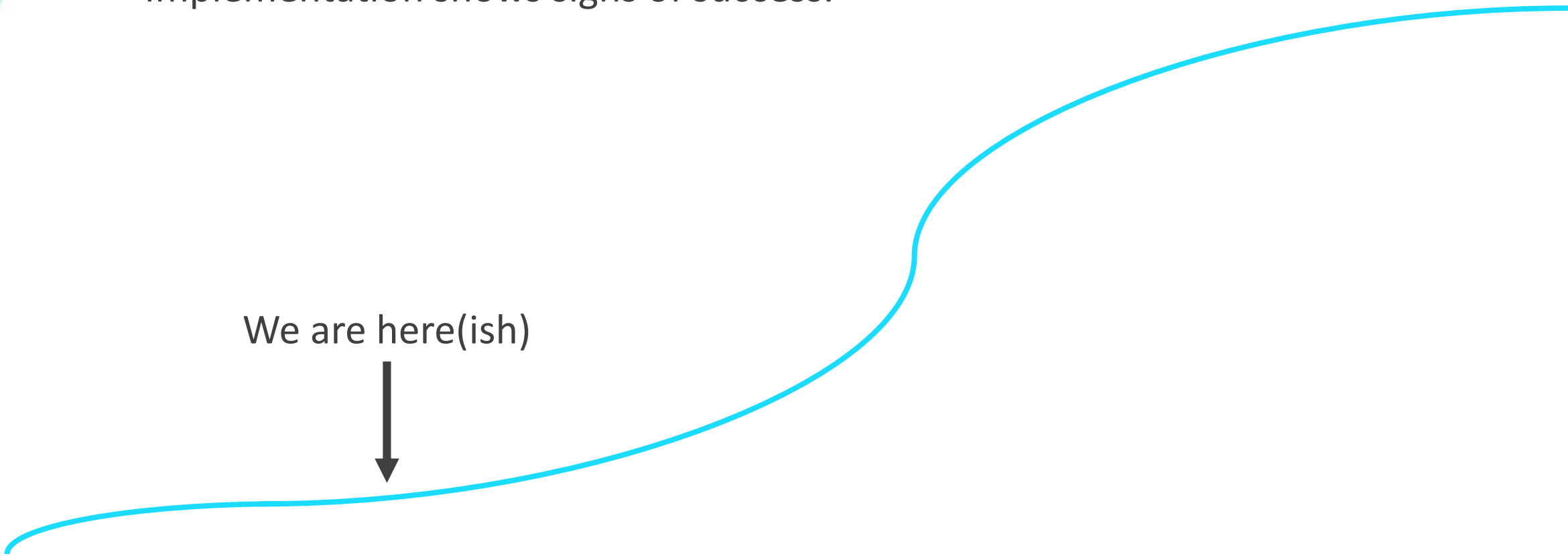
establish government as an early adopter

Connect.gov: baked in PETs; transition to IOC;
5 credential providers; 5 agencies


NIST
DEPARTMENT OF HUMAN SERVICES
ID
IDESG
GTRI
PROBLEM. SOLVED.
SAFRAN
MorphoTrust USA
TSCP
TRANSGLOBAL SECURE COLLABORATION PROGRAM
HealthIDx
Daon
INTERNET
iD
GSMA
CRITERION systems
AAMVA

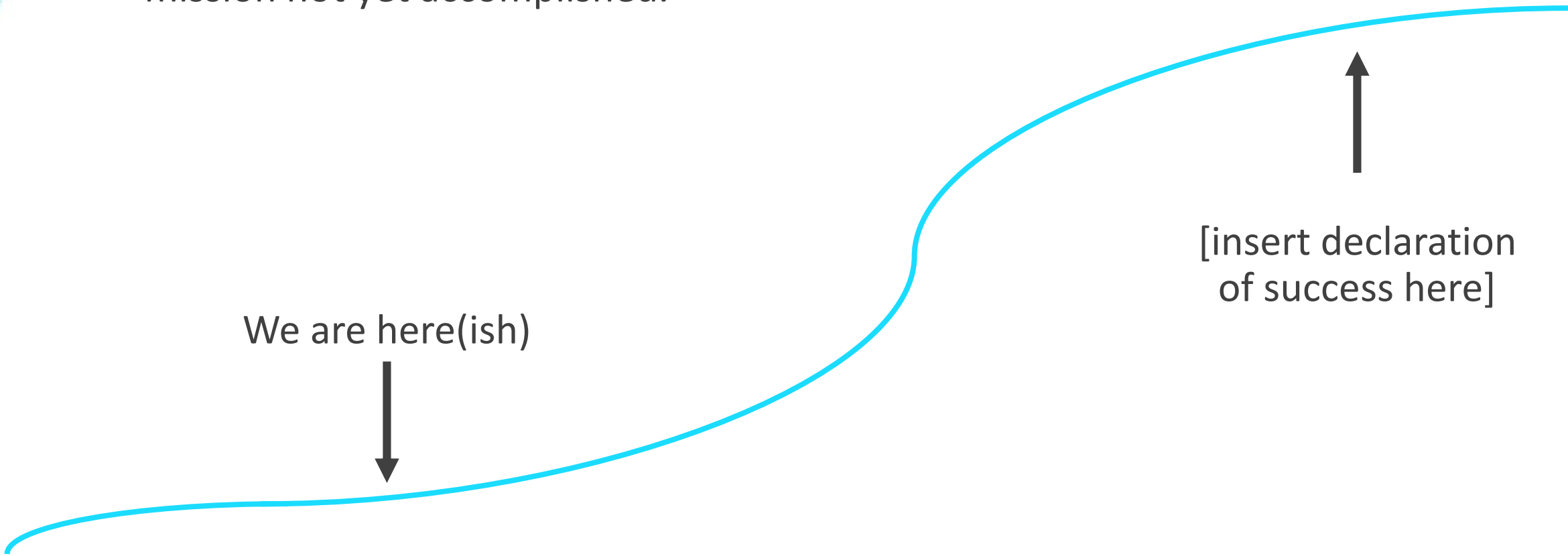
IT’S 2016.

Implementation shows signs of success.

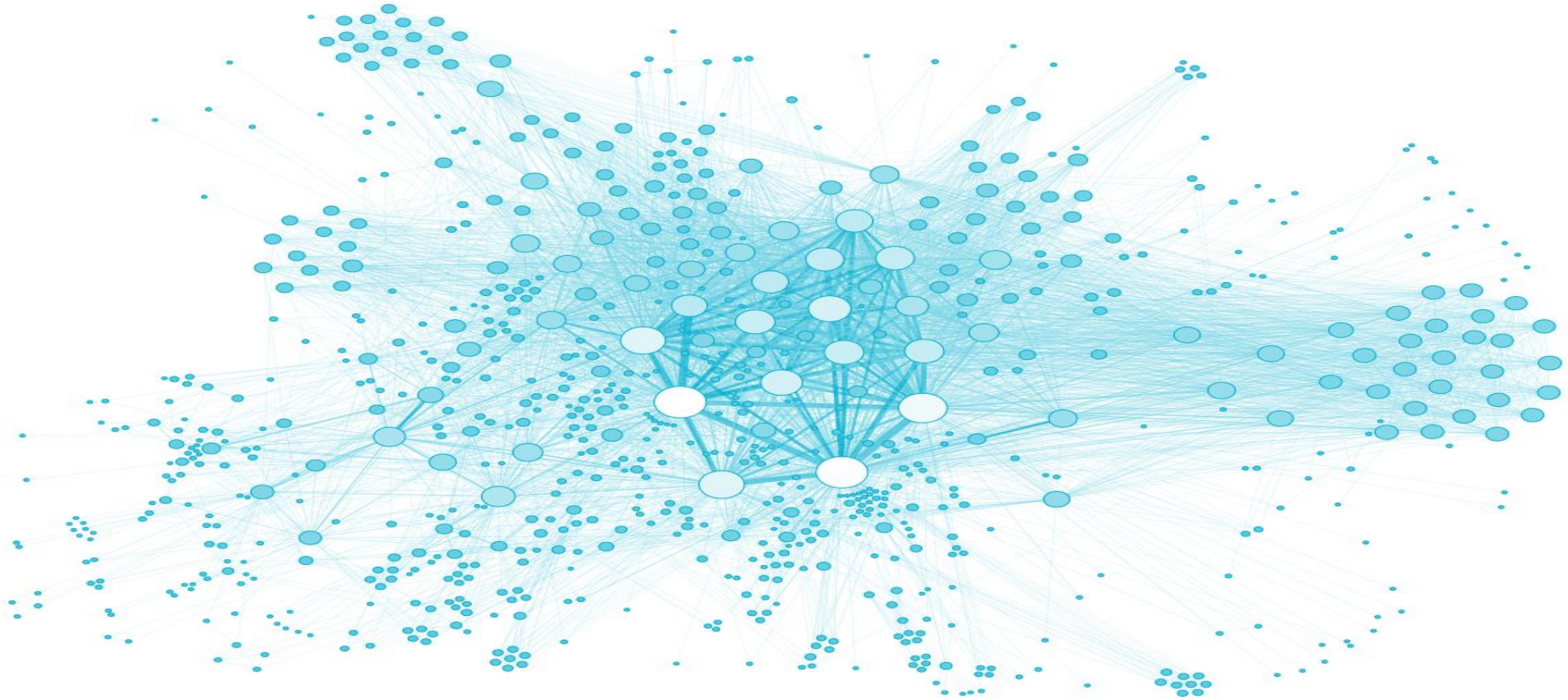


IT’S 2016.

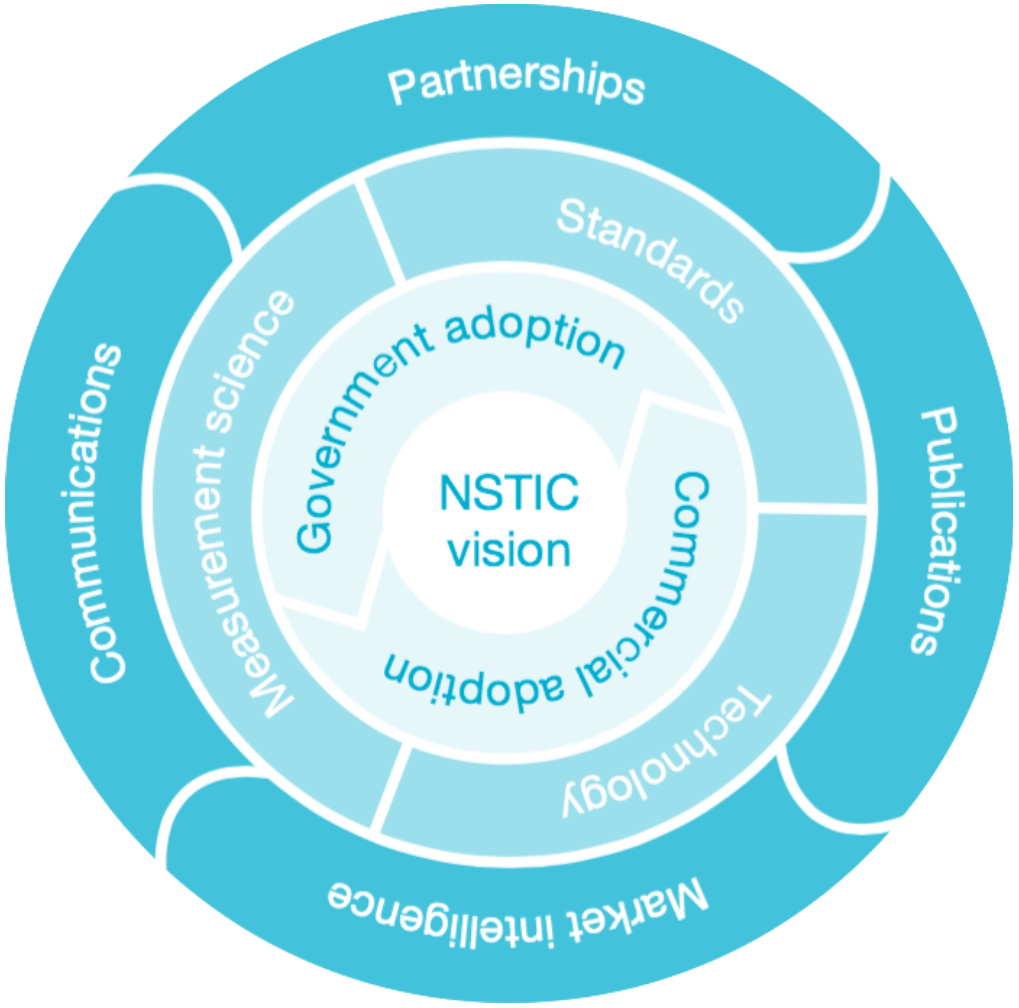
mission not yet accomplished.



WE MUST ACCELERATE ADOPTION



THE MODEL: PART 2



evolve and sustain
the Identity Ecosystem

SMARTER ENGAGEMENT TO SOLIDIFY THE MARKET

more technical deep dives
more high level, public awareness

communications

foster a more coherent community
establish global reach

partnerships

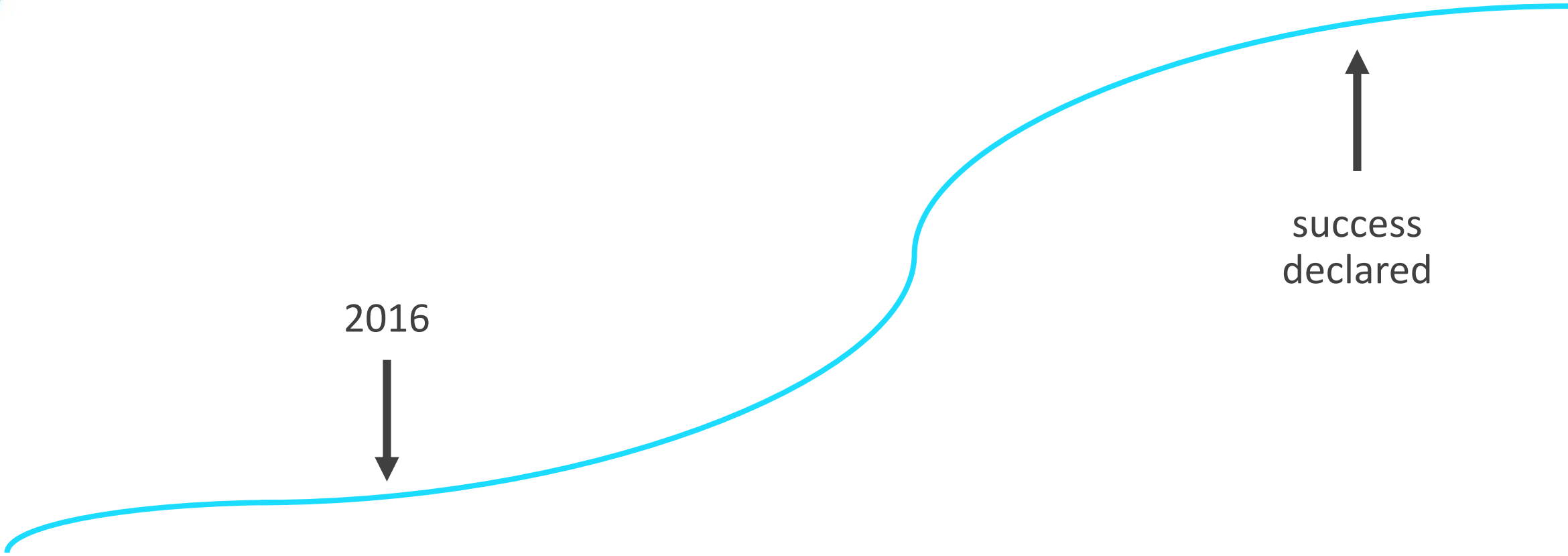
market intelligence

track and share market trajectory
strategically direct investment

publications

seek U.S., global, and industry alignment
Invest in what market won't support

IT’S 2021.



NSTIC FEDERATED IDENTITY IN HEALTHCARE PILOT PROGRAM

PURPOSE AND SCOPE

PURPOSE OF 2016 SOLICITATION

- Pilot online identity solutions that embrace and advance the NSTIC vision of an identity ecosystem.
- Fund innovative solutions that would otherwise not occur in the marketplace.
- Demonstrate the usage of federated online identity solutions for patients and providers across multiple healthcare providers.
- Provide the foundation for potential best practices guidance to other healthcare providers.

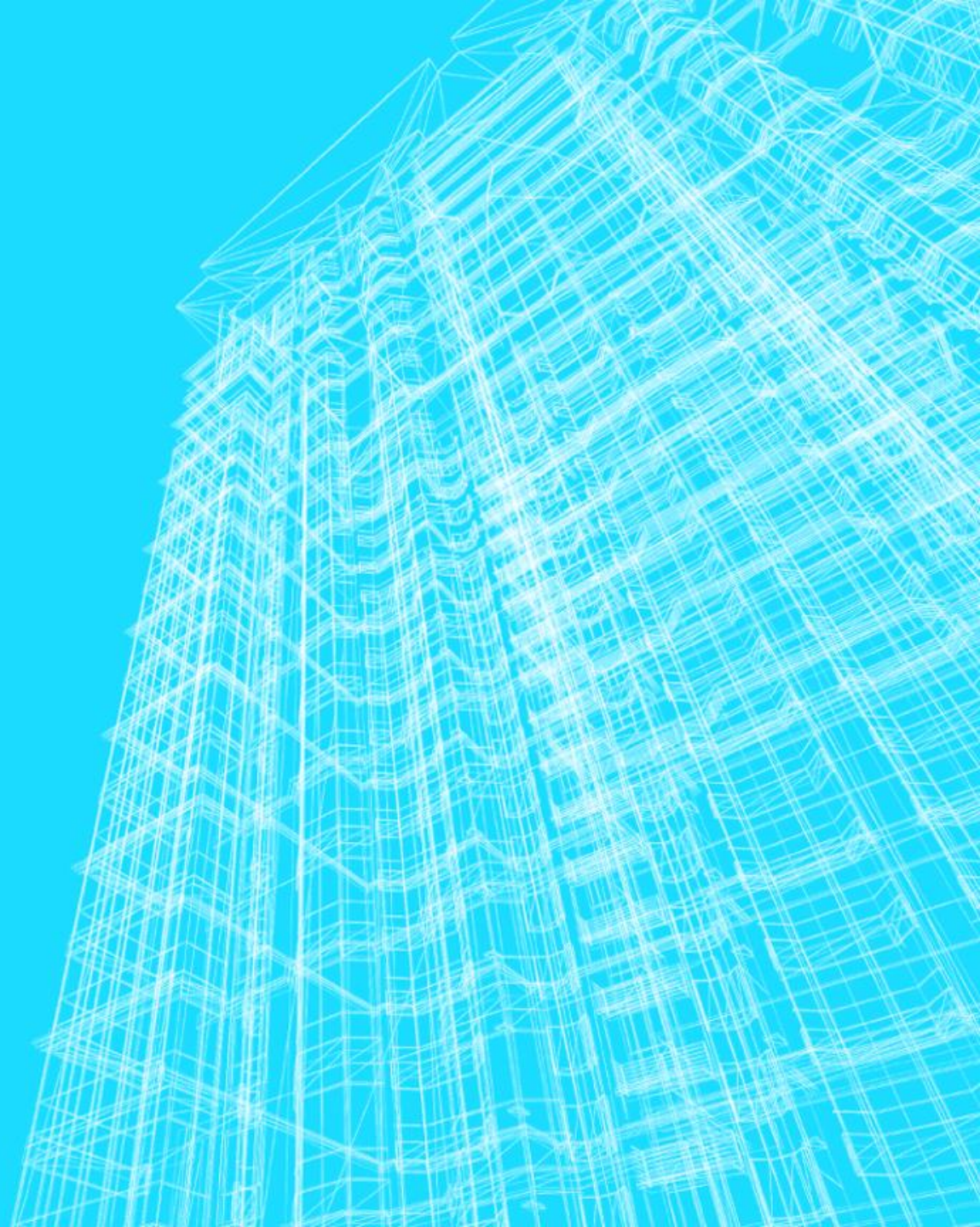
PROPOSED IDENTITY SOLUTIONS MUST

- 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.
- Enable online access to at least two organizationally separate healthcare organizations.
- Demonstrate that the federated credential solution aligns with the Identity Ecosystem Framework Requirements.
- Allow for interoperability with other identity federations in the healthcare sector and, where possible, other sectors.
- Include collecting metrics and other information about the implementation of the federated credential solution that can contribute to a best practices guidance document.

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.
- help catalyze the adoption of federated identity credentials in the healthcare sector.

ELIGIBILITY



WHO IS AN ELIGIBLE APPLICANT?

- 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)

➡ located in the United States and its territories

PARTNERING IS REQUIRED

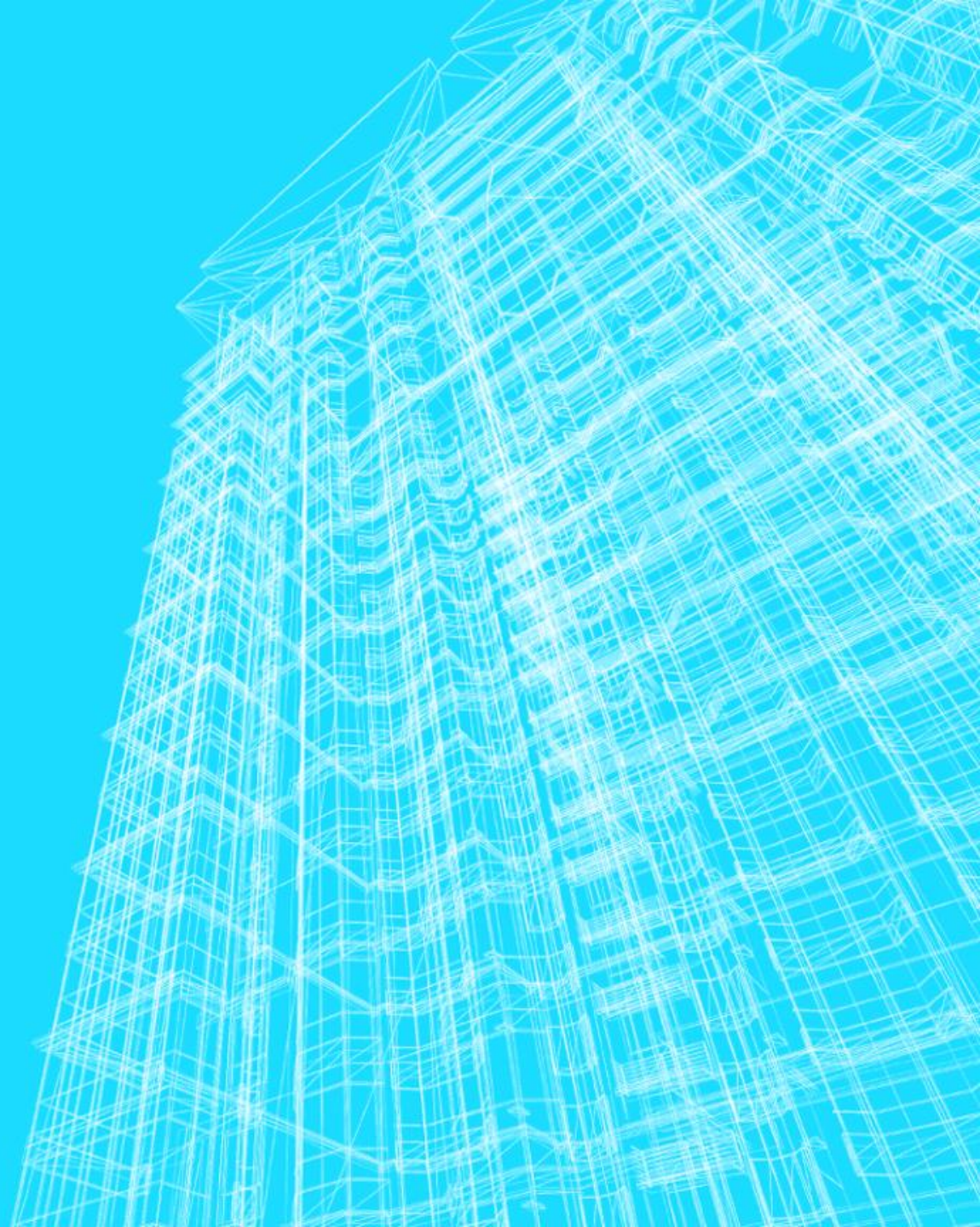
- Applicants must partner with at least one other healthcare organization in their locality/region.
- The partner organization should have anticipated overlap with the applicant organization of patients, physicians and other clinical staff (such as a physician practice group(s), clinic(s) and hospital(s)).

PARTNERING IS REQUIRED

- The partner organization must be
  - organizationally independent of the applicant and
  - maintain a separate health information system from the applicant.

APPLICATION CONTENTS AND EVALUATION CRITERIA

FULL APPLICATIONS



APPLICATION CONTENTS – FULL APPLICATION

- SF-424, Application for Federal Assistance
- SF-424A, Budget Information - Non-Construction Programs
- SF-424B, Assurances - Non-Construction Programs
- CD-511, Certification Regarding Lobbying
- SF-LLL, Disclosure of Lobbying Activities (if applicable)

APPLICATION CONTENTS, CONTINUED

- Full Technical Application
  - Word-processed document
  - No more than twenty-five (25) pages
  - Responsive to program description and evaluation criteria
  - Contains the following:
    - Executive Summary
    - Problem Statement and Use Cases
    - Federated Identity Solution
    - Metrics Collection
    - Statement of Work and Implementation Plan
    - Qualifications
- Budget Narrative
- Indirect Cost Rate Agreement (*if applicable*)
- Letters of Commitment
- Resumes
- Data Management Plan (*if applicable*)

PROBLEM STATEMENT AND USE CASES

- The specific use cases (e.g., provider and patient) to be piloted including
  - Specific separate organizations participating in each use case
  - Size of the populations at each organization
  - Any special characteristics of the populations

FEDERATED IDENTITY SOLUTION

- Description of chosen solution
- Technical architecture including architecture and data flow diagrams
- Solution should leverage readily available commercial identity credentials and products to the extent possible
- 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

METRICS COLLECTION

- Description of the plans to collect metrics for at least a six-month period of the operational pilot.
- Present the specific metrics to be collected.
- Collected metrics should include, at minimum, pre- and post-operational pilot.

STATEMENT OF WORK AND IMPLEMENTATION PLAN

- 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.

QUALIFICATIONS

- Information on the qualifications, proposed roles, and level of planned effort of the project participants
- One individual from each participant, with details of committed participation
- Project manager or project leader with demonstrated experience leading projects of similar size and complexity
- At least one subject matter expert in addressing usability of the type of system envisioned for the project and the beneficiary population

PRIVACY EXPERT QUALIFICATIONS

- Specialized knowledge of both privacy technology and policy issues
- At least 5-7 years' experience in a cross-set of privacy and information technology skills
- May an employee of the applicant, consultant or employee of a contractor or subawardee
- Experience may be demonstrated by education, certifications, and job skills
- Qualifications could include certifications such as CIPT or CIPM, 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
- Less preferably, this role could be filled by multiple individuals with complementary skillsets and experience, but must provide plan for how they will work together

LETTERS

- Required Letter of Commitment from a partner healthcare organization to participate in the pilot

RESUMES

Two page resumes for the following positions are outside the page count and required for all of the following:

- Project Manager
- Technical Lead
- Usability Expert
- Privacy Expert
- Key person from each pilot participant

EVALUATION CRITERIA

- Privacy-enhancing Capabilities (12 points)
- Strength of Identity Proofing Approach (12 points)
- Strength of Authentication Approach (12 points)
- Supports Standards for Interoperability (12 points)
- Ease of use(12 points)
- Project Impact (15 points)
- Quality of Implementation Plan (15 points)
- Resource Availability (10 points)

PRIVACY-ENHANCING CAPABILITIES (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.

STRENGTH OF IDENTITY PROOFING APPROACH (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.

STRENGTH OF AUTHENTICATION APPROACH (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.

SUPPORTS STANDARDS FOR INTEROPERABILITY (5 POINTS)

Reviewers will evaluate how well the proposed solution complies with or leverages widely adopted interoperability standards and specifications, as appropriate, such as:

- Fast Identity Online (FIDO) (https://fidoalliance.org/specifications/overview/)
- Security Assertion Markup Language (SAML) (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)
- OpenID Connect (http://openid.net/connect/)
- 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/).

EASE OF USE (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.

PROJECT IMPACT (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.

QUALITY OF IMPLEMENTATION PLAN (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;

QUALITY OF IMPLEMENTATION PLAN, CONTINUED

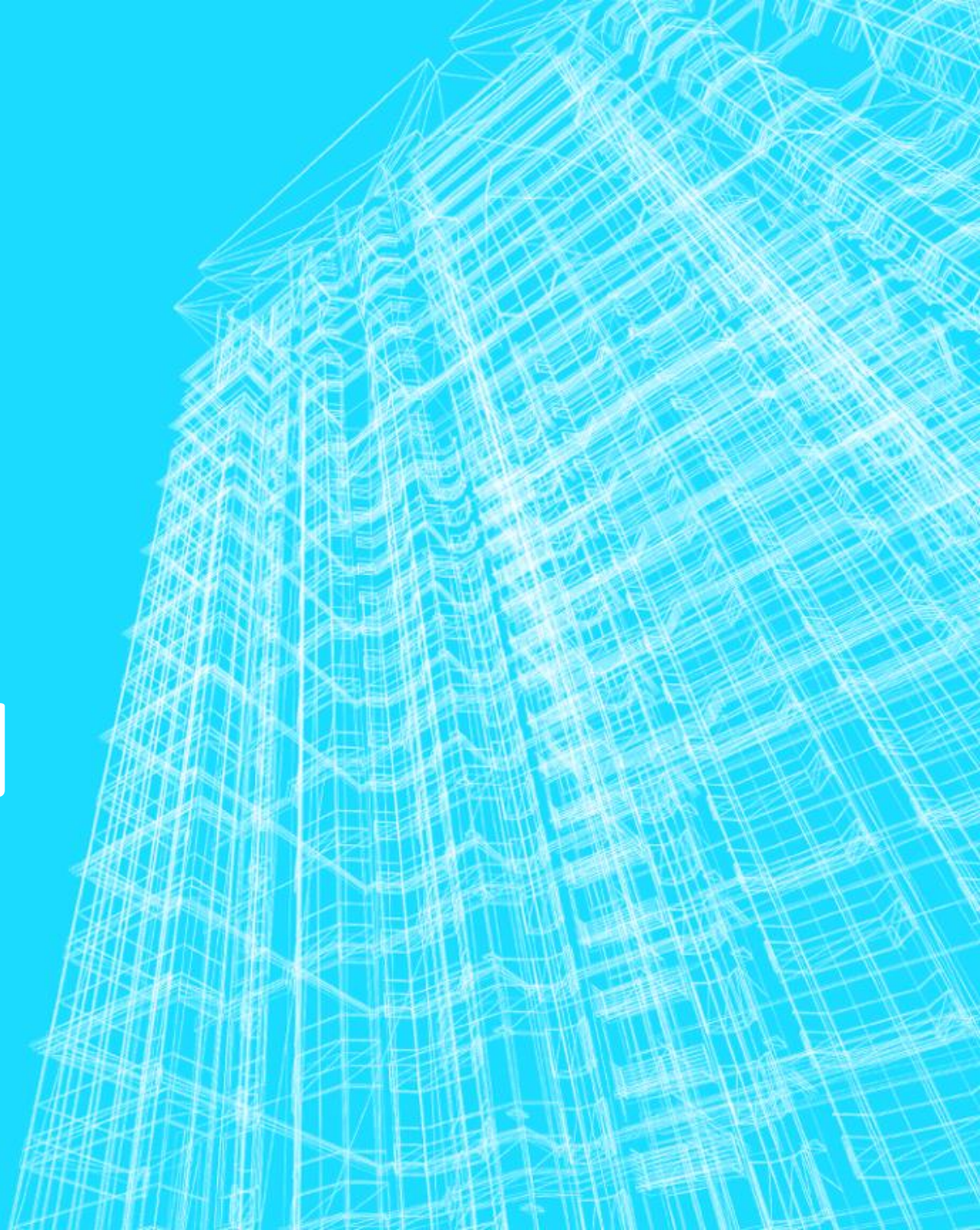
- The quality of the project leadership's plans to manage the project including managing the work of all project participants including sub-recipients, contractor's, etc., to ensure realization of project goals and objectives;
- The appropriateness of the measurable milestones; and
- The timeline for including at least six months of metrics collection on the active pilot.

RESOURCE AVAILABILITY (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.

DUE DATE, FUNDING, APPLICATION SUBMISSION, AND EVALUATION AND SELECTION PROCESS



DUE DATES AND SCHEDULE

- Applications due Wednesday, June 1, 2016
- Earliest anticipated start date is September 1, 2016

APPLICATION SUBMISSION

- All applications must be submitted through Grants.gov.
  - **Verify that your registration is up to date early!**
  - **SAM requires annual registration renewal!**

- Hardcopy, email or faxed applications will not be accepted.

FUNDING

- $750K to $1 million may be made available in FY 2016
- Project is expected to be 18 months including 6 months of metrics collection
- Only one award may be made
- 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

APPLICATION EVALUATION PROCESS – FULL APPLICATIONS

- Administrative Review
  - Eligibility
  - Completeness
  - Responsiveness to the Scope
- Technical Review
  - Using Evaluation Criteria
  - At least three independent reviews
- Evaluation Panel uses review scores to determine competitive range
- Questions may be sent to and/or webinars held with competitive applicants
- Evaluation Panel re-reviews application with additional information
- Selection made using reviews and selection factors

SELECTION FACTORS

a. The availability of Federal funds;

b. Whether the project duplicates other projects funded by NIST, DoC, or by other Federal agencies;

c. Diversity of the portfolio of NSTIC projects and alignment with NSTIC priorities.

ADMINISTRATIVE REQUIREMENTS

DEAN IWASAKI
NIST GRANTS SPECIALIST

CONTENTS

GENERAL RULES OF THUMB…

Budget Format

- Separate Budget by project year so that work and the associated costs are clearly definable/associated with the available funding for that year.
- Costs should be placed under the applicable budget categories of Personnel, Fringe Benefits, Travel, Equipment, Supplies, Contractual, Other, and Indirect Charges.
- The total dollar amounts listed under each budget category in the Budget Narrative must match the dollar amounts listed on the SF424A.
- Cost computations and written justification must be provided for all costs in the Budget Narrative.
- The Budget Narrative and SF424A should only include the Federal share of costs. Cost share is not required.
- Best estimates are acceptable.
- The Budget and scope are subject to negotiation and amendment, if selected for funding.

BUDGET NARRATIVE CONTENT

a. Personnel

- Name or TBD
- Job title
- Role of individual and description of work to be performed
- Salary
- Level of effort (in hours or percentage of time)
- Total cost to project

* Consultants/contracted personnel should be listed under the Contractual budget category.

* Include sufficient time for personnel to complete reporting requirements and participate in public forums that help to develop the Identity Ecosystem Framework, such as the IDESG.

BUDGET NARRATIVE CONTENT

b. Fringe Benefits

- Identified separately from salaries and wages.
- Based on rates determined by organizational policy.
- Costs included as fringe should not be charged under another cost category.

c. Travel

- Include: destination; travel dates or duration of trip; names of travelers or number of people traveling; transportation rate, lodging rate, subsistence rate (per diem); and description of how travel is directly related to the project.
- For travel that is yet to be determined or destinations that are not known, provide best estimates based on prior experience.
- Include travel to two Identity Ecosystem Steering Group meetings annually.

BUDGET NARRATIVE CONTENT

d. Equipment

- Defined as: property with an acquisition cost of $5,000 or more (unless the organization has established lower levels) and expected service life of more than one year.
- Items that do not meet the threshold for “equipment” may be placed under the Supplies budget category.
- Identify each piece of equipment, the cost, and provide a description of how it will be used and why it is necessary for the successful completion of the project.
- Prorate costs for equipment that will be used for other purposes besides project-related effort.

e. Supplies

- Identify each supply item, and provide a breakdown of costs by quantity or unit of cost.
- Describe the necessity of the cost for the completion of the project.

BUDGET NARRATIVE CONTENT

f. Contractual

- Treat each contract or subaward as a separate line item.
- Describe the services provided and their purpose.
- Describe the necessity of the contract or subaward.
- Describe how costs were determined
- For contracts, identify if the contract is sole sourced or competed.

BUDGET NARRATIVE CONTENT

Contracts vs. Subawards

The primary distinction between a sub-recipient and a vendor is the performance of programmatic work.

Sub-recipient

- Performs substantive portion of the programmatic work
- Involved in the design and conduct of the project
- Usually on cost-reimbursement
- Flow-through of OMB/CFR and award requirements
- No fee or profit can be charged on the grant for subrecipients

Vendor

- Provides the goods and services within normal business operations
- Provides similar goods or services to many different purchasers
- Operates in a competitive environment
- Not subject to Federal programmatic compliance requirements
- Profit can be charged

Subaward

An award of financial assistance made under an award by a recipient to an eligible sub-recipient or by a sub-recipient to a lower tier sub-recipient (DoC Grants Manual).

Contract (via a Vendor/Procurement)

Principal purpose of the relationship is the acquisition by purchase, lease, or barter, of property or services (DoC Grants Manual).

BUDGET NARRATIVE CONTENT

g. Construction

- Not an allowed cost under this program.

h. Other Direct Costs

- Costs that do not easily fit into the other cost categories.
- Identify the cost, and provide a breakdown of the cost by quantity or unit of cost.
- Describe the necessity of the cost for the completion of the project.

BUDGET NARRATIVE CONTENT

j. Indirect Charges

- Indirect costs include business expenses that are not readily identified, but are necessary for general operation and conduct of activities.
- Indirect cost rates are negotiated with the recipient's cognizant Federal agency.
- For applicants without a negotiated rate:
  - Use best estimates for a rate to be negotiated with NIST, or
    - For DoC General Indirect Cost Rate Program Guidelines for Grantee Organizations, July 2013, email Dean Iwasaki, NIST Grants Specialist, at dean.iwasaki@nist.gov.
  - Use the 10% De Minimis Rate, authorized by 2 CFR 200.414.

ALLOWABLE COSTS

- Reasonable
- Allocable
- Allowable under grant terms, regulations, statute
- Necessary for the performance of the award
- Consistently charged regardless of source of funds

ALLOWABLE COSTS

- Direct costs for technical work
  - Salaries of technical personnel on the project
  - Equipment used on the project (pro-rated)
  - Materials and supplies
- Travel to Identity Ecosystem Steering Group meetings
- Award related audits - audits will be required by an external auditor (CPA or cognizant Federal audit agency), as specified in the Special Award Conditions in the Award Notice
- Accounting system certification - if a recipient has never received Federal funding, a certification that indicates whether the recipient has a functioning financial management system meeting the provisions of 2 CFR 200.302 may be required from a CPA. Sample will be provided at time of award.

UNALLOWABLE COSTS

- Profit and Fees
- Application Writing/Development
- Contingency Fees
- Any cost disallowed by 2 CFR Part 200 and 48 CFR Part 31, if applicable
- Any cost not required for the approved work

AWARD REQUIREMENTS

- 2 CFR 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, as adopted by the Department of Commerce at 2 CFR 1327.101 (http://go.usa.gov/SBYh and http://go.usa.gov/SBg4)
- DoC Financial Assistance Standard Terms and Conditions, December 26, 2014 (http://go.usa.gov/hKbj)
- Special Award Conditions specific to NSTIC and each specific cooperative agreement

PAYMENT OF GRANT FUNDS

- Award funds are paid electronically through the Automated Standard Application for Payment (ASAP) system managed by the US Treasury.

- Enrollment will be required if not already enrolled.

REPORTING REQUIREMENTS

- **SF425 Federal Financial Reports**
  - 30-days after the end of each calendar quarter.
  - Final 90-days after the end of the award.
- **Performance (Technical) Reports**
  - 30-days after the end of each calendar quarter.
  - Final 90-days after the end of the award.
  - Guidance on content will be provided by NPO.
- **Biannual Progress Reporting to NSTIC Steering Group**
- **Patent and Property Reports**
  - Patent reports (use iEdison.gov) and property reports, as needed.

REPORTING REQUIREMENTS - INTELLECTUAL PROPERTY

- Covered by “Department of Commerce Financial Assistance Standard Terms and Conditions”
- Follows Bayh-Dole Act
- “The recipient has the right to own any invention it makes … The recipient may not assign its rights to a third party without the permission of DOC unless it is to a patent management organization (i.e., a university’s Research Foundation). The recipient’s ownership rights are subject to the Government’s nonexclusive paid-up license and other rights.” (DoC, Financial Assistance Standard Terms and Conditions, D.03)

REPORTING REQUIREMENTS - AUDITS

- States, Local Governments, Non-Profits follow 2 CFR Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.
- Commercial Organizations follow the DoC Financial Assistance Standard Terms and Conditions, December 26, 2014 or Special Award Conditions in the award package.
- Recipients should budget for audit costs as needed.

QUESTION & ANSWER SESSION