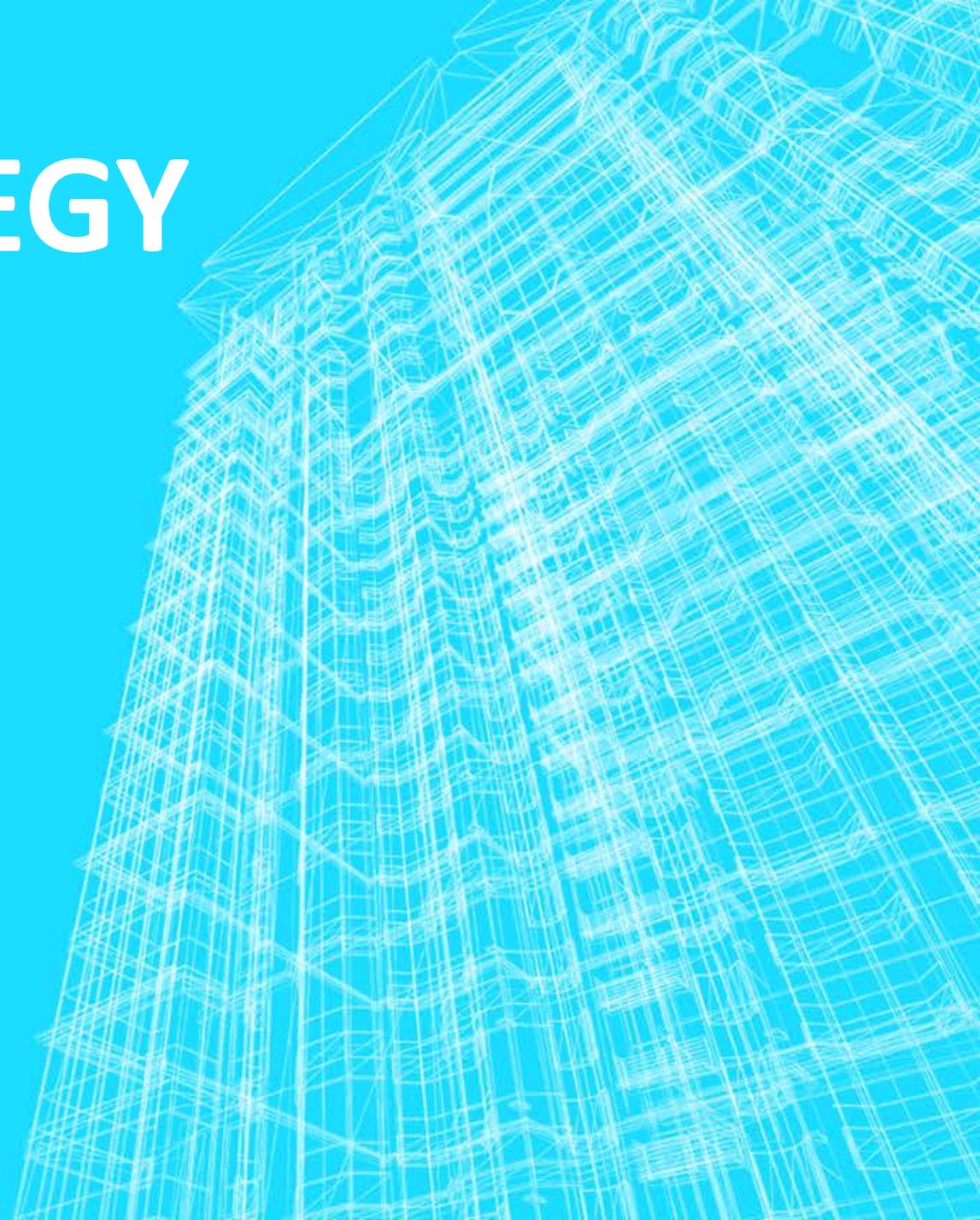


# NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE APPLICANTS WEBINAR

JANUARY 7, 2016

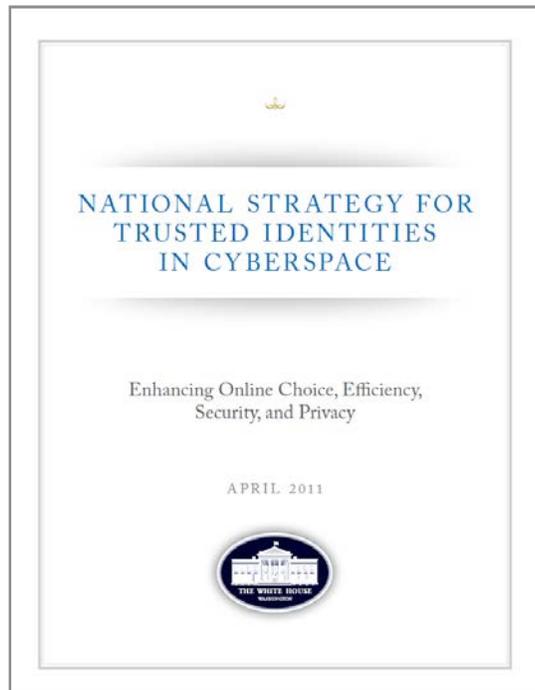


# **NSTIC OVERVIEW AND STATUS UPDATE**

**MICHAEL GARCIA**  
NSTIC ACTING DIRECTOR



# NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE



White House initiative (April 2011)

**NSTIC Goal:** Catalyze the marketplace so we can choose from a variety of new types of solutions to use in lieu of passwords for online transactions that are more secure, convenient, and privacy-enhancing.

# HOW NSTIC STARTED...

## Identity Ecosystem Steering Group (IDESG):

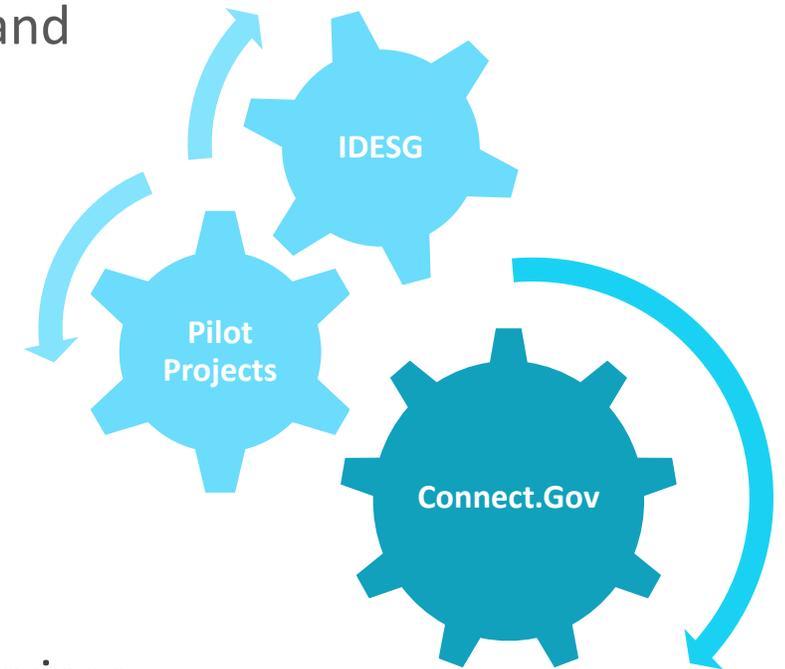
- A privately-led group across sectors furthering the NSTIC vision to develop a more secure, private, and easy-to-use online environment for all

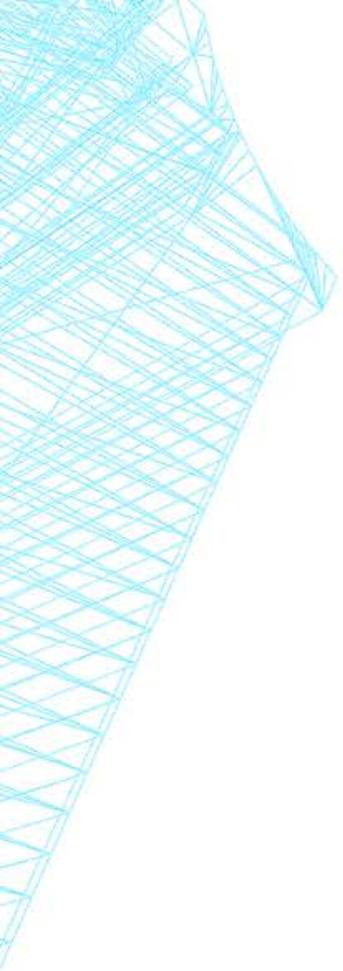
## Pilot Projects:

- Catalyzing a marketplace of solutions and infrastructure

## Connect.Gov (formerly FCCX):

- Creates a secure, privacy-enhancing service that conveniently connects people to government services and applications online using an approved digital credential they may already have and trust





## NSTIC GOALS OF TODAY...

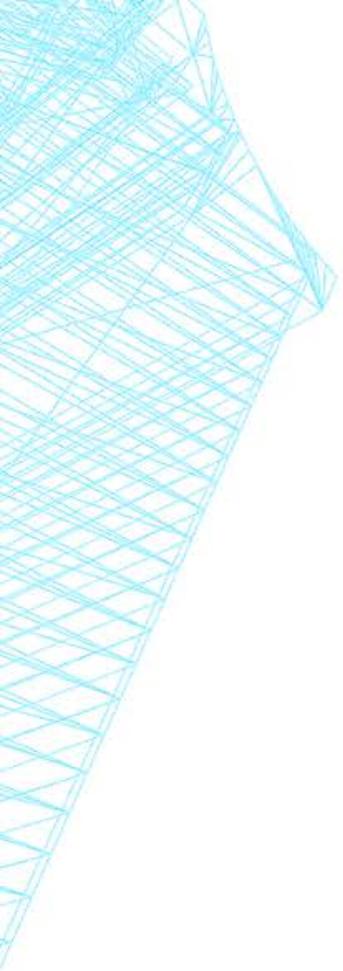
Advance measurement science, technology, and standards adoption in identity management through:

- Increased **federal adoption** of trusted digital identity solutions
- Increased **commercial adoption** of trusted digital identity solutions

We are advancing privacy-enhancing and interoperable identity solutions to promote a vibrant identity ecosystem!

# IDENTITY IS CENTRAL TO...





# IMAGINE IF...

Four years from now, 80% of your customers arrived at websites already holding a secure credential for identification and authentication – and sites could trust this credential in lieu of existing username/password systems.

- Interoperable with your login system (you don't have to issue credentials)

- Strong authentication (no more password management)

- Tied to a robust identity proofing mechanism (you know if they are who they claim to be – if you need to know)

- Baked-in rules with clear liability and privacy protection

## WHY NSTIC?

There is a marketplace today – but there are barriers the market has not yet addressed on its own.

Government can serve as a convener and facilitator—and a catalyst.



# WHAT DOES THE NSTIC CALL FOR?

## **Private sector will lead the effort**

- Not a government-run identity program
- Private sector is in the best position to drive technologies and solutions...
- ...and ensure the Identity Ecosystem offers improved online trust and better customer experiences

## **Federal government will provide support**

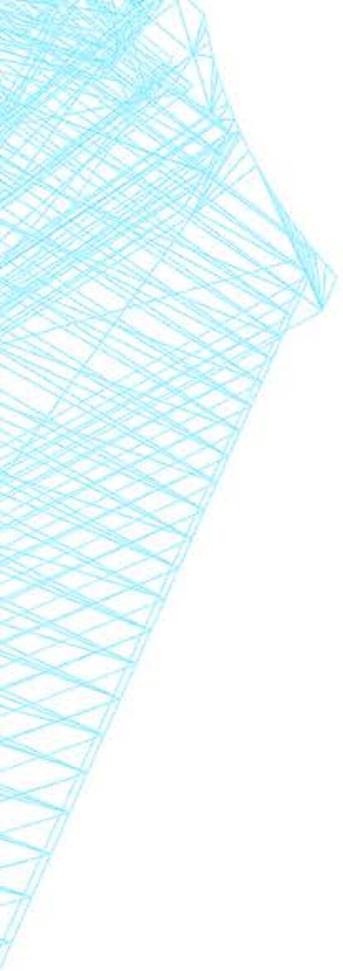
- Help develop a private-sector led governance model
- Facilitate and lead development of interoperable standards
- Provide clarity on national policy and legal issues (i.e., liability and privacy)
- Fund pilots to stimulate the marketplace
- Act as an early adopter to stimulate demand

## OUR ULTIMATE GOAL...

Catalyze the marketplace – so that all Americans can soon choose from a variety of new types of solutions that they can use in lieu of passwords...

...for online transactions that are more secure, convenient and privacy-enhancing.

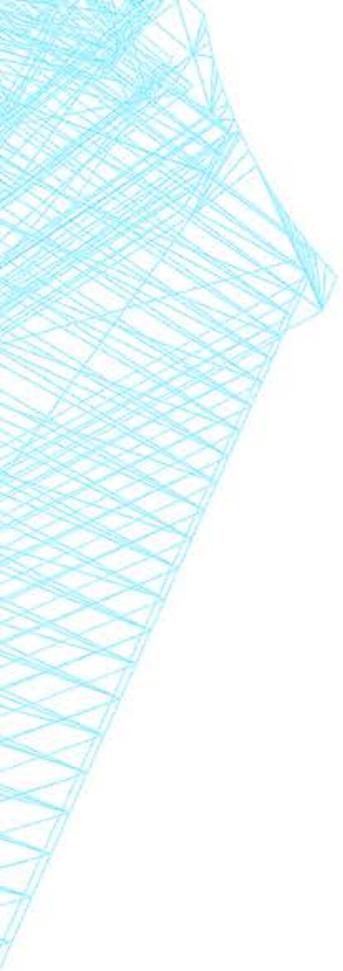




# ABOUT THE NSTIC NATIONAL PROGRAM OFFICE

Charged with leading day-to-day coordination across government and the private sector in implementing NSTIC

Steady funding at \$16.5M in FY12, FY13, FY14 and FY15, FY16



# KEY IMPLEMENTATION STEPS

## Convene the Private Sector

- August 2012: Launched privately-led **Identity Ecosystem Steering Group (IDESG)**; Funded by NIST grant, IDESG tasked with crafting standards and policies for the Identity Ecosystem Framework <http://www.idecosystem.org/>
- October 2013: IDESG incorporates as 501(c)3, prepares to raise private funds
- Fall 2015: Released the Identity Ecosystem Framework
- Spring 2016: Launch a self-attestation program for the Identity Ecosystem Framework

## Fund Innovative Pilots to Advance the Ecosystem

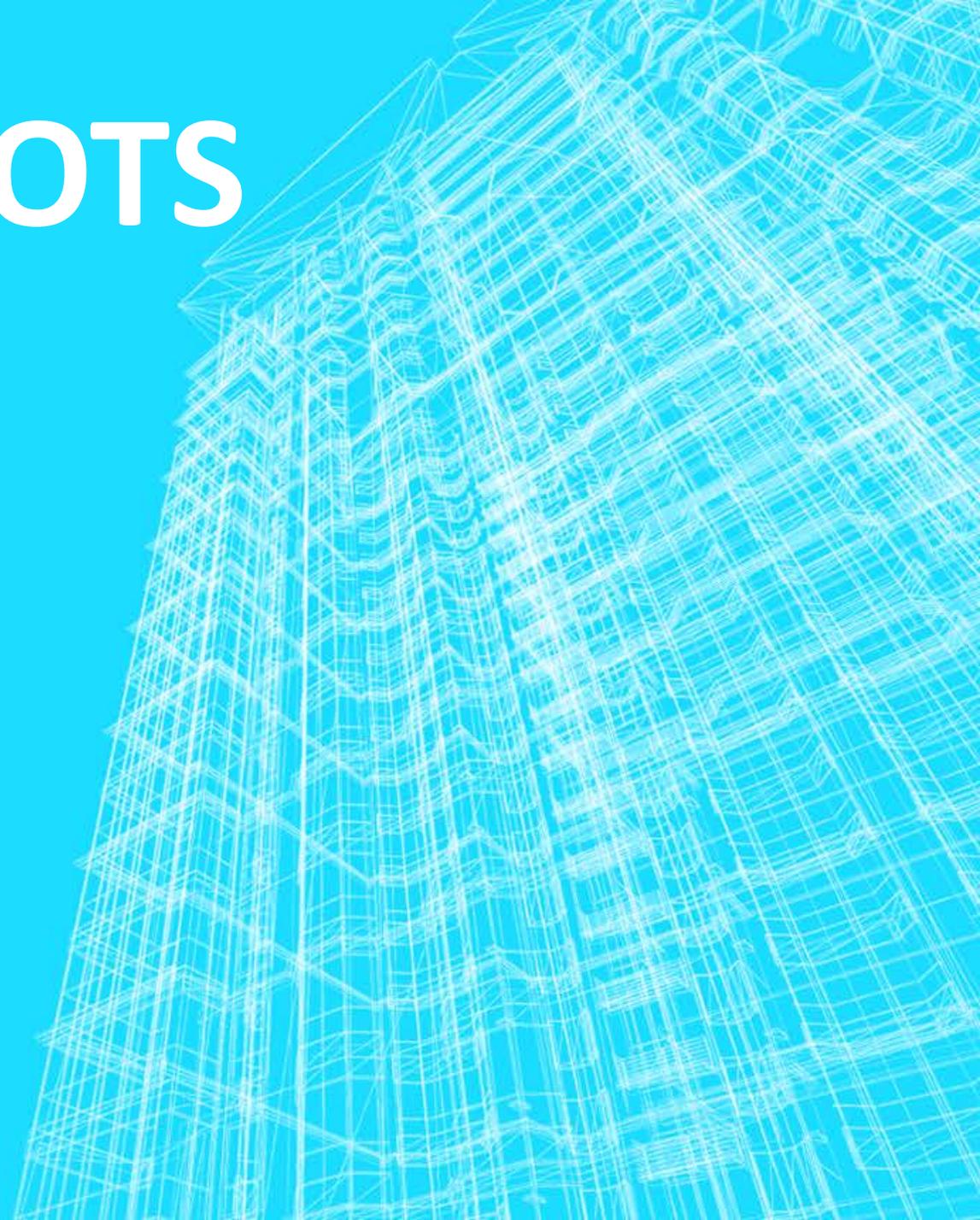
- Four rounds of **pilot grants** in 2012, 2013, 2014 and 2015 worth \$35 million total
- **Includes two awards in 2013 for State Pilots Cooperative Agreement Program**
- Solicitations took a challenge-based approach focused on addressing barriers the marketplace has not yet overcome

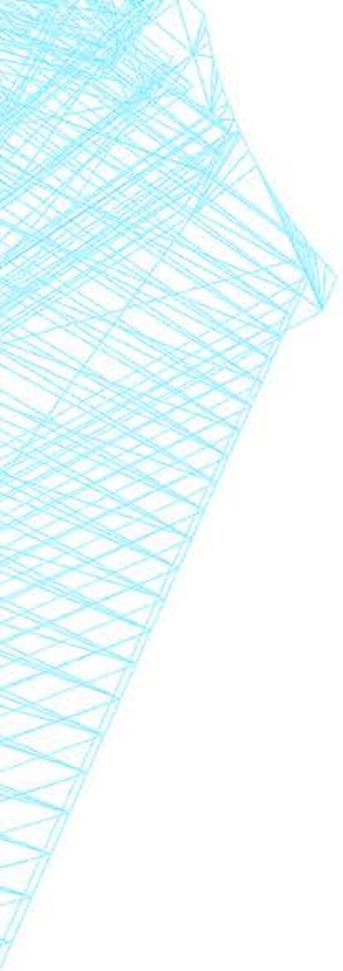
## Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the **Federal Identity, Credential, and Access Management (FICAM) Roadmap**
- White House effort to create a Federal Cloud Credential Exchange (formerly FCCX – now Connect.gov)
- August 2013: USPS awards FCCX/**Connect.gov** contract

# INSTANT STATE PILOTS COOPERATIVE AGREEMENT PROGRAM

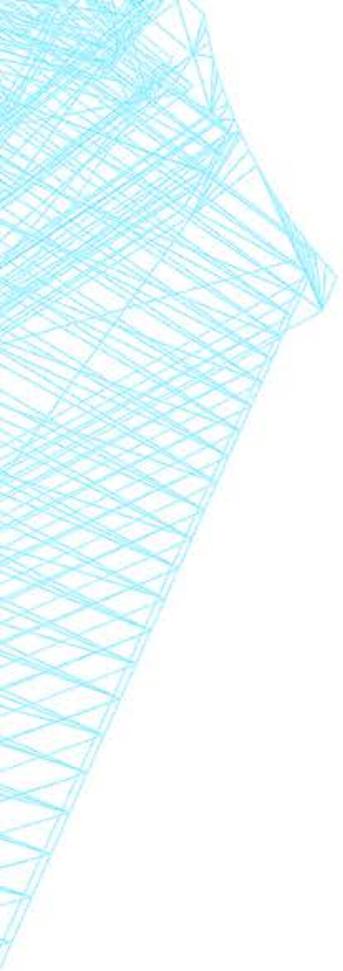
PURPOSE AND SCOPE





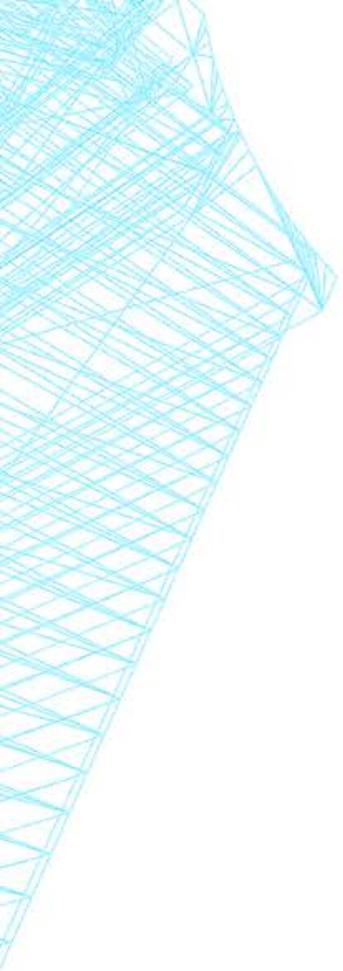
## PURPOSE OF 2016 SOLICITATION

- 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.
- Deploy pilots to test or demonstrate new solutions that are not widely adopted today.



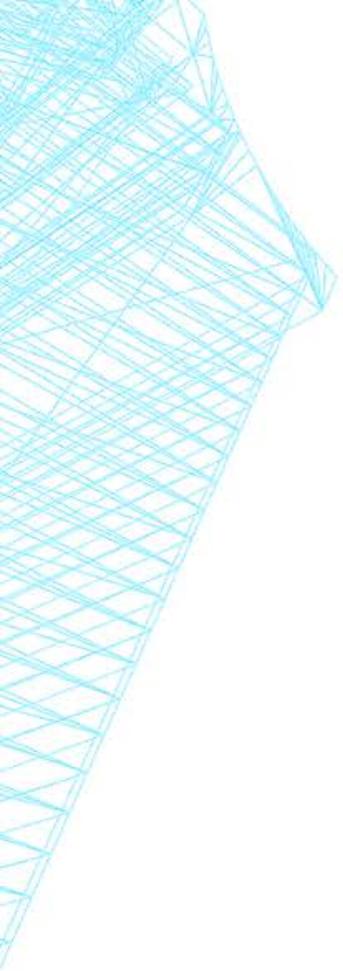
# PROPOSED IDENTITY SOLUTIONS MUST

- Enable online access to one or more state, local, or tribal government service(s).
- Provide for a federated, verified identity that enables multi-factor authentication and an effective identity proofing process meeting the risk needs of the service(s).
- Align with the Identity Ecosystem Framework Requirements.
- Allow for interoperability with other federations in use in the public and private sectors.



# BARRIERS TO STRONG ONLINE CREDENTIALS FOR GOVERNMENT SERVICES:

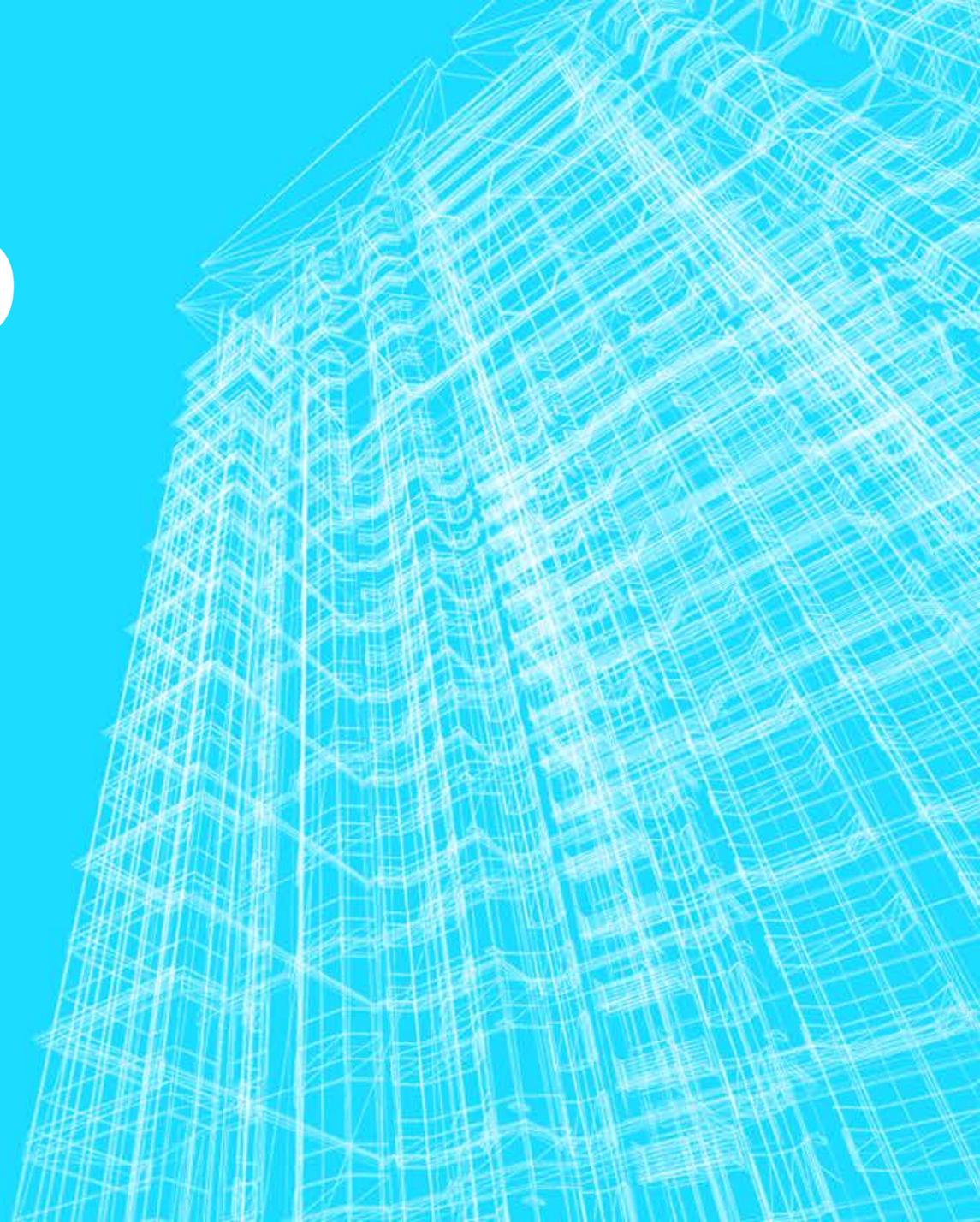
- Concerns about applicant and beneficiary privacy, including risks that arise from the crossing of contextual boundaries and the capacity for more tracking and profiling of individuals.
- Difficulties conducting effective identity proofing and ensuring coverage of the full beneficiary population.
- Concerns that the identity management process may place additional burdens on the target audience and increase barriers to accessing services.
- Lack of implementations of alternative identity proofing methods beyond knowledge-based approaches.
- Balancing transparency to individual users and ease-of-use especially of strong authentication technologies.

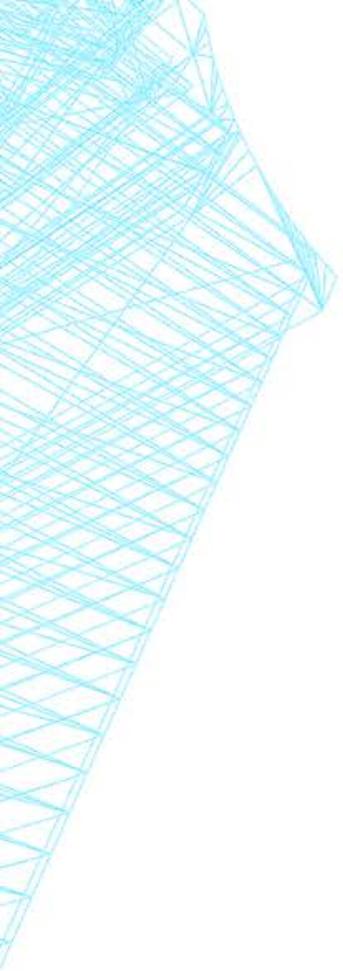


## A FOCUS ON BARRIERS

- Looking for innovative solutions to overcoming these barriers
- Best projects are likely to address most or all of the barriers
- Priority given to projects using a private provider that demonstrates the potential for interoperability with both state and Federal programs
- Goal is to encourage partnerships between private sector providers and all levels of government

# DUE DATES AND SCHEDULE





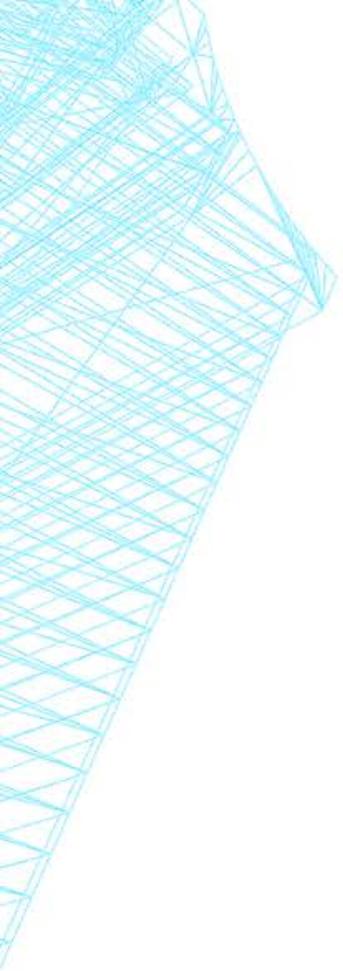
## DUE DATES AND SCHEDULE

- Abbreviated applications due Thursday, February 18, 2016
- Responses to applicants by Friday, March 25, 2016
- Full applications due Wednesday, May 25, 2016
- Earliest anticipated start date is September 1, 2016

# APPLICATION CONTENTS AND EVALUATION CRITERIA

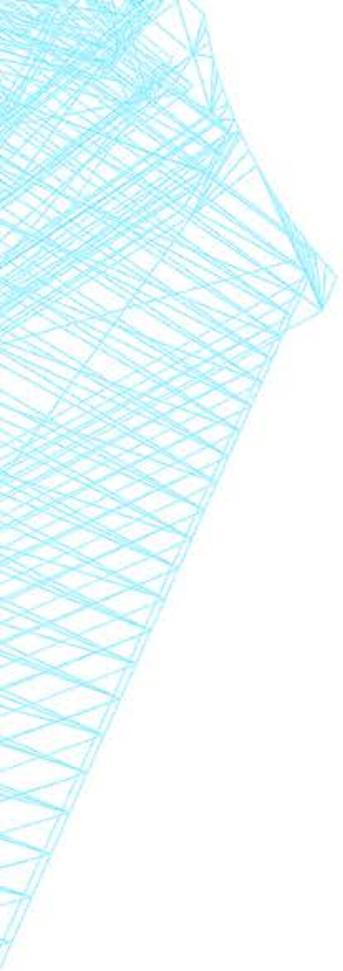
ABBREVIATED APPLICATIONS





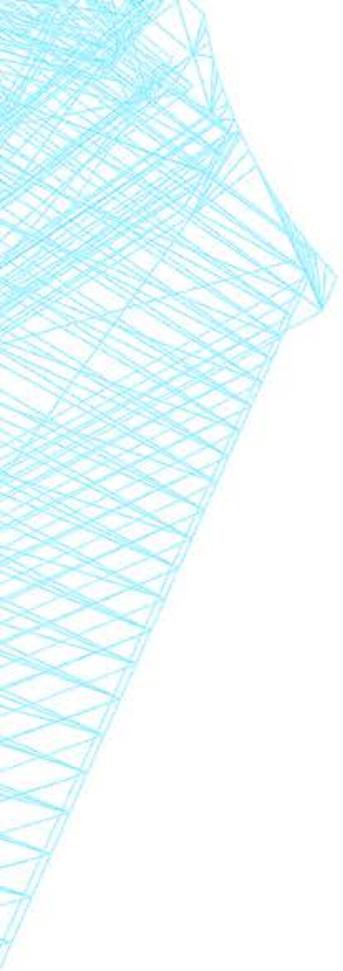
# APPLICATION CONTENTS – ABBREVIATED APPLICATION

- SF-424, Application for Federal Assistance
- Abbreviated Proposal – Maximum four pages
- For projects not led by an eligible government entity – letters of interest from two state, local or tribal government entities



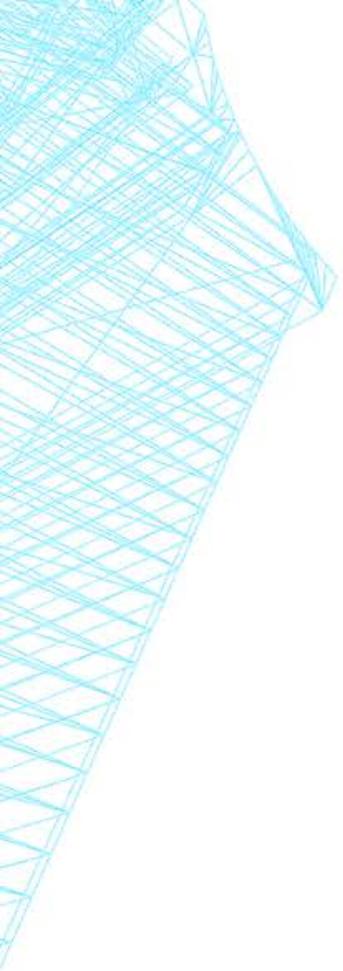
# ABBREVIATED PROPOSAL – CONTENTS

- Sufficient information to determine if the project is within scope
- Explain how the planned identity solution will:
  - Provide for a federated, verified identity that enables multi-factor authentication that meets the risk needs of the service(s);
  - Provide for an effective identity proofing process that meets the risk needs of the service(s);
  - Show alignment to the Identity Ecosystem Framework requirements;
  - Enable online access to at least two state, local, or tribal government services; and
  - Allow for interoperability with other federations in use in the public and private sectors.



# EVALUATION CRITERIA – ABBREVIATED APPLICATIONS

1. Includes an effective identity proofing process (0 to 30 points). Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's approach to identity proofing.
2. Enables multi-factor authentication (0 to 30 points). Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's approach to enabling multifactor authentication.



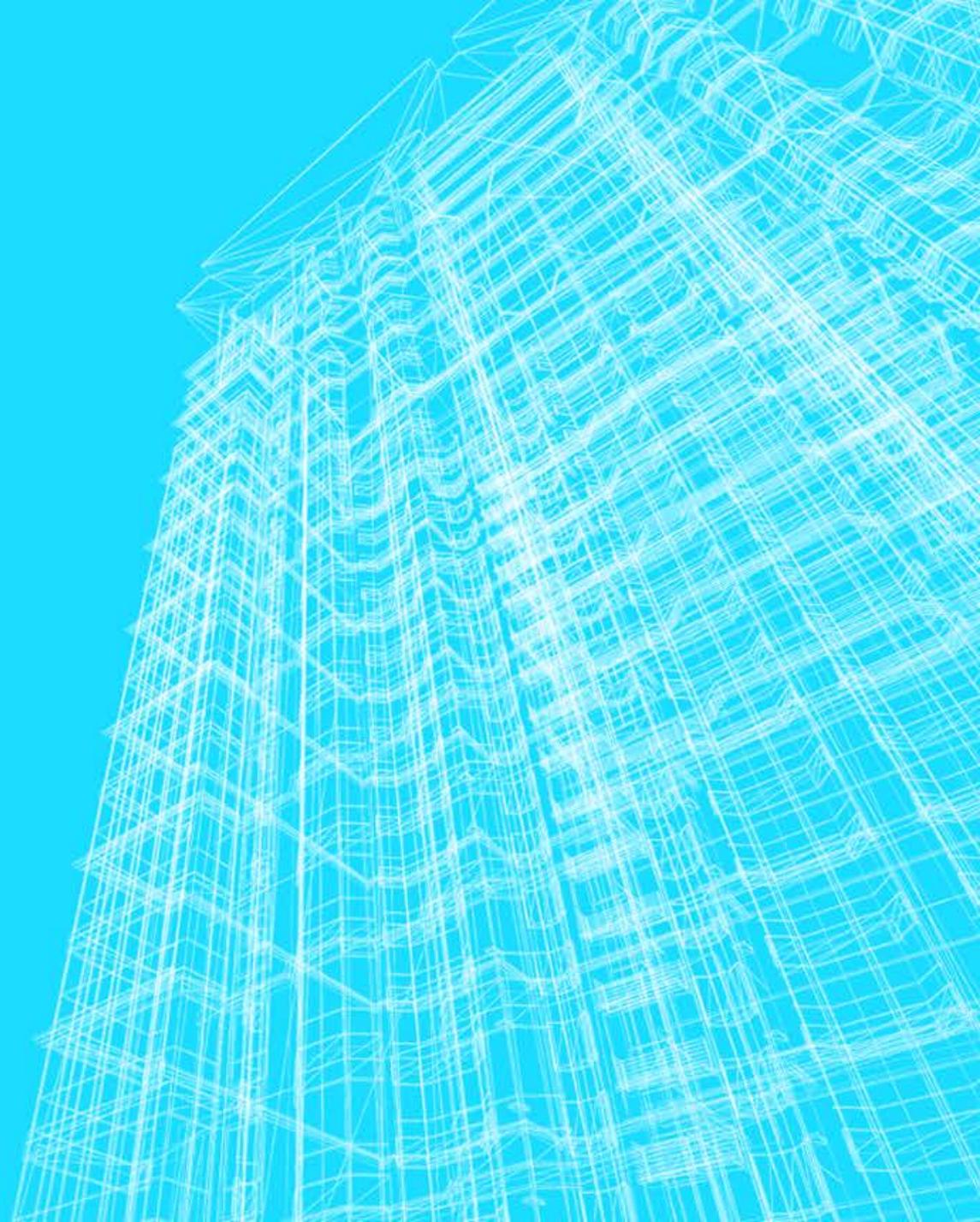
# EVALUATION CRITERIA – ABBREVIATED APPLICATIONS

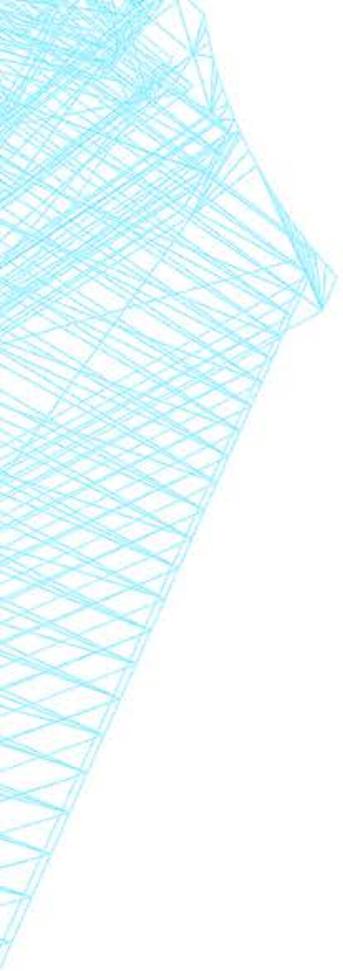
3. Aligns with the Identity Ecosystem Framework Requirements (0 to 35 points). Reviewers will evaluate how well the applicant's proposed solution aligns with the IDEF requirements.

4. Allow for interoperability with other federations in use in the public and private sectors (0 to 5 points). Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's approach to ensuring interoperability with other federated digital identity approaches.

# APPLICATION CONTENTS AND EVALUATION CRITERIA

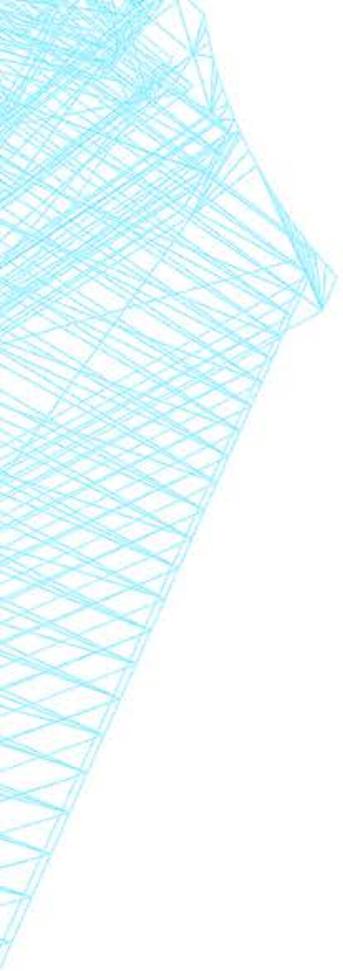
FULL APPLICATIONS





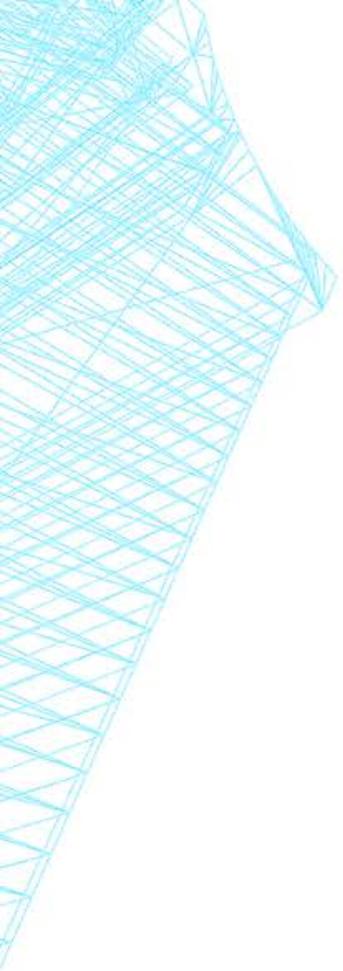
# APPLICATION CONTENTS – FULL APPLICATION

- SF-424, Application for Federal Assistance
  - Same as for abbreviated application
- SF-424A, Budget Information - Non-Construction Programs
  - Budget should reflect anticipated expenses for each year of the project of no more than three (3) years, considering all potential cost increases, including cost of living adjustments.
- SF-424B, Assurances - Non-Construction Programs
- CD-511, Certification Regarding Lobbying
- SF-LLL, Disclosure of Lobbying Activities (if applicable)



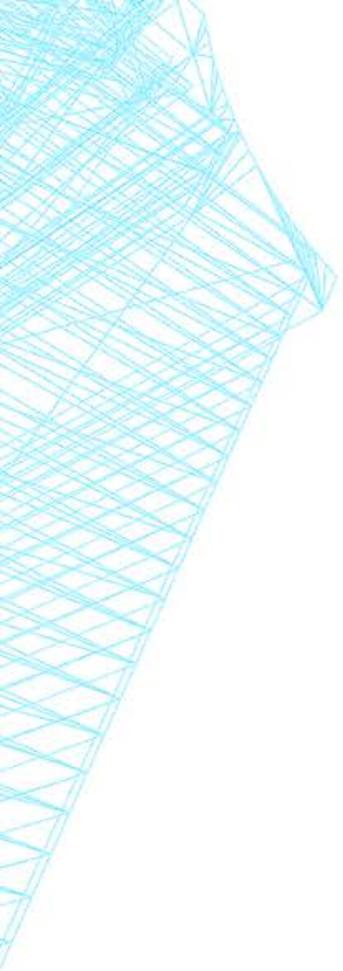
# APPLICATION CONTENTS, CONTINUED

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



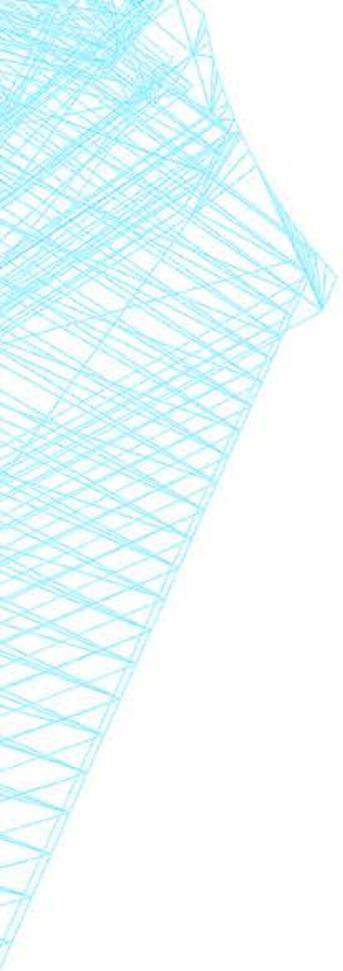
# PROBLEM STATEMENT AND USE CASES

- The specific use cases to be piloted including
  - Specific government programs involved
  - Characteristics of the beneficiary populations
  - Size of the beneficiary population
- The solution that this project would introduce to the marketplace and what would otherwise occur without the project
- Any special characteristics of the government program(s) involved including any waivers needed from Federal offices



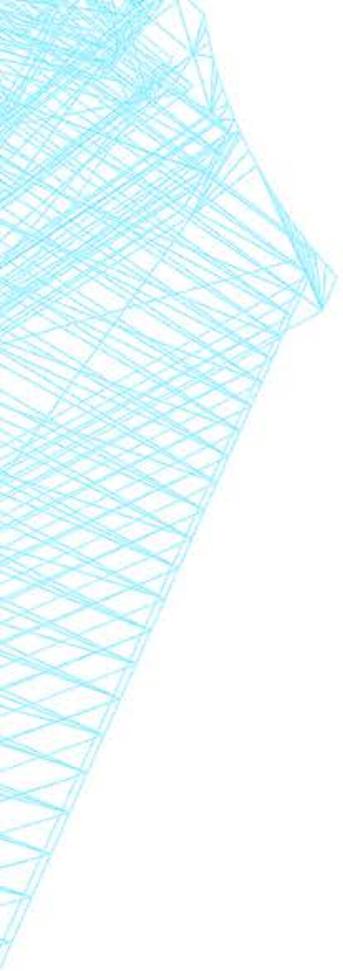
# TECHNICAL ARCHITECTURE

- Technical architecture for the proposed operational pilot
- Information on all the components of the solution(s), how these components interconnect, and what information is exchanged among the components
- Architecture diagram and data flow diagrams
- Explain how the technical and policy measures are applied in a risk-based approach to address privacy concerns
- Mapping to the IDESG's Identity Ecosystem Framework requirements (*optional*)



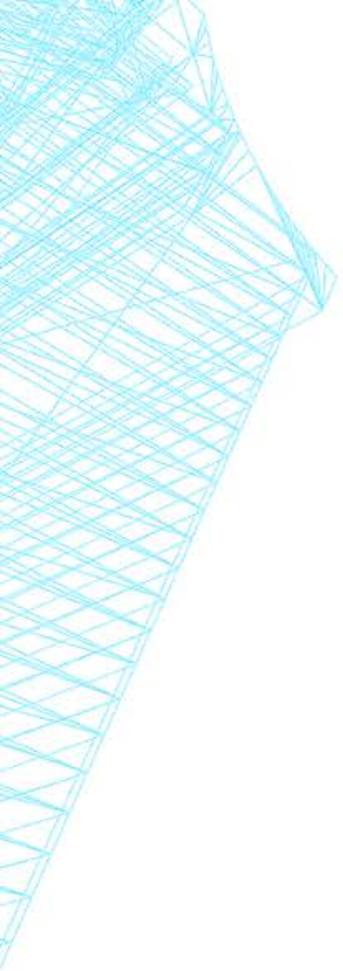
# STATEMENT OF WORK AND IMPLEMENTATION PLAN

- Measurable performance objectives with metrics used to determine the success
- Specific proposed tasks and schedule;
- Schedule of measurable events and realistic, measurable milestones including any state budget authorization actions required and Federal waivers required;
- Project management plans including managing the work of all project participants, including sub-recipients, contractors, etc.
- Approach to ensure the project results will align to the IDESG's IDEF.
- Can include a Gantt chart, Work Breakdown Structure or other format to present plan which is not included in the page count
- Can include a detailed analysis of privacy risks which is not included in the page count



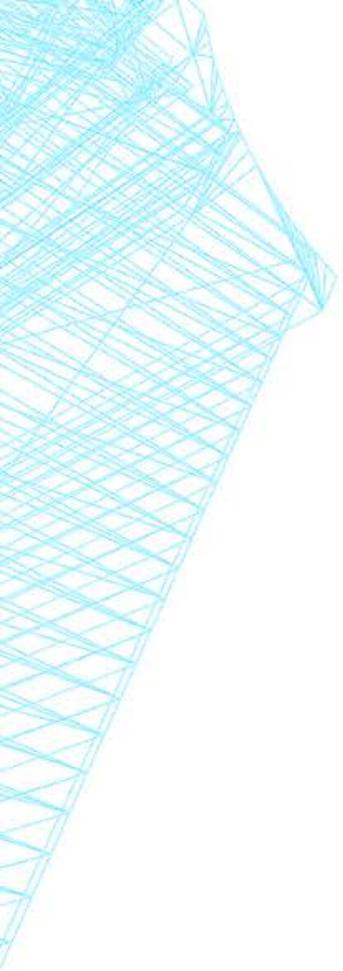
## PROJECT IMPACT

- Plans to scale the pilot project into full production and self-sustaining, large scale use.
- Project participants' planned role(s) in organizations developing the Identity Ecosystem Framework
- Planned efforts to disseminate information and reach out to users
- Planned uses of the solution beyond the initial benefit programs



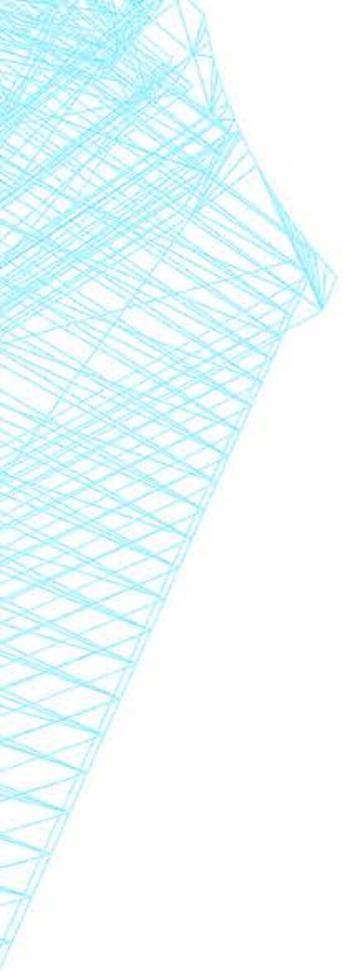
# QUALIFICATIONS

- 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.



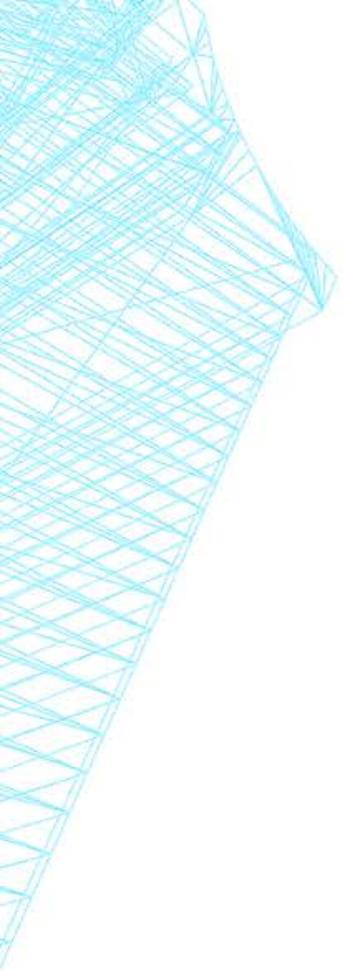
# PRIVACY EXPERT QUALIFICATIONS

- 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

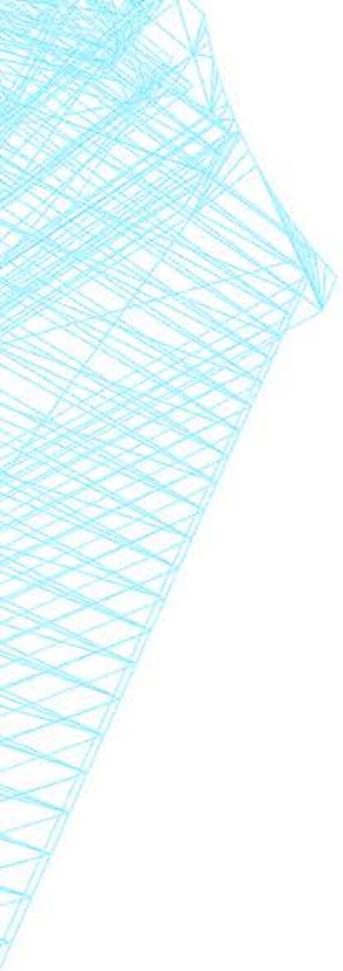
- Letters of commitment to participate from third parties indicating their commitment to participate and what they will do:
  - Subawardees
  - Contractors
  - Other collaborators
- Letters are outside the page count
- For projects not led by government entities, letters of commitment are required from two state, local or tribal government entities



# RESUMES

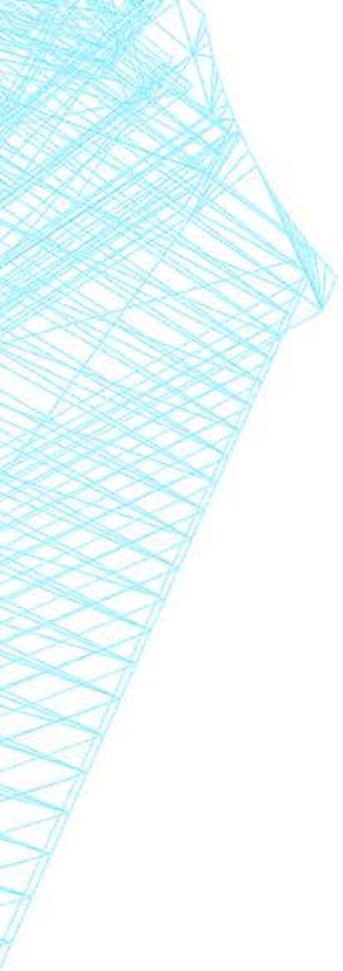
Two page resumes for the following positions are outside the page count and required for all of the following:

- Project Manager
- Technical Lead
- Usability Expert
- Privacy Expert



# EVALUATION CRITERIA

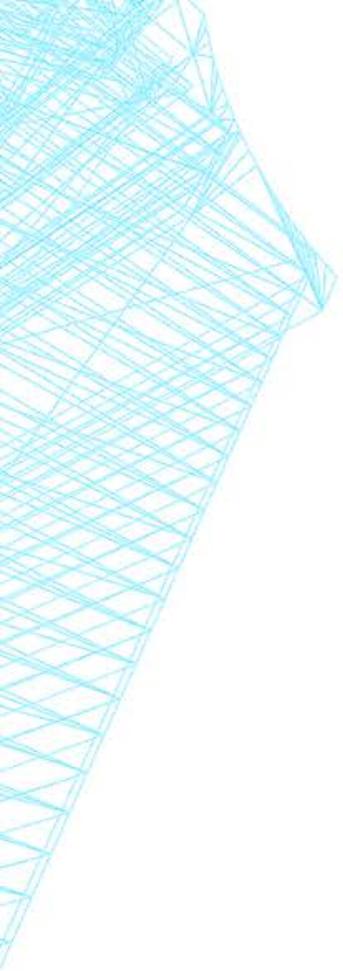
- Quality of the Planned Technical Solution (60 points)
  - a) Privacy-enhancing Capabilities (15 points)
  - b) Strength of Identity Proofing Approach (15 points)
  - c) Strength of Authentication Approach (15 points)
  - d) Supports Standards for Interoperability (5 points)
  - e) Usability Across Total Population (10 points)
  
- Quality of Implementation Plan (20 points)
  
- Contribution to Identity Ecosystem (10 points)
  
- Resource Availability (10 points)



# PRIVACY-ENHANCING CAPABILITIES (15 POINTS)

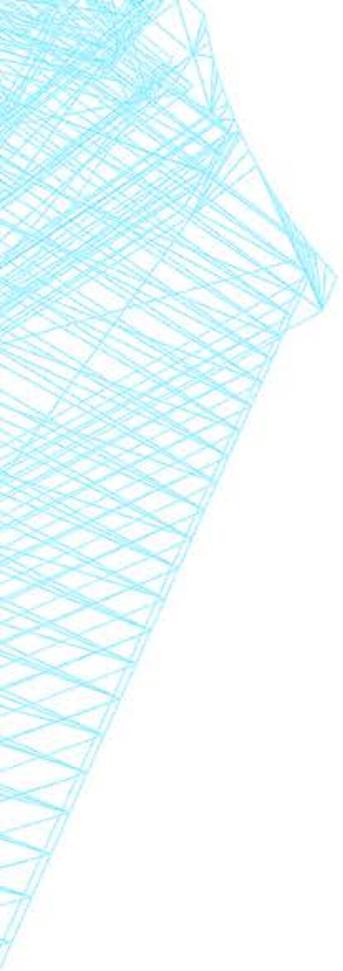
Reviewers will evaluate how well the applicant's proposed solution exhibits privacy-enhancing capabilities including:

- The manner in which it enables individuals and other pilot participants to have reliable assumptions about the personal information being processed by project participants (the project lead, contractors, subawardees and other collaborators);
- The manageability 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;
- The manner in which personal information or events can be processed without association or the potential for association with individuals beyond operational requirements; and
- The controls implemented to mitigate privacy and civil liberties risks, including whether policy or technical measures are used for each risk, and why any, in any given case, (i) a policy measure is more appropriate than a technical measure and (ii) the project participant implementing the control is more appropriate than another project participant;



# STRENGTH OF IDENTITY PROOFING APPROACH (15 POINTS)

Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's proposed approach to leverage a secure and reliable method of identity proofing.



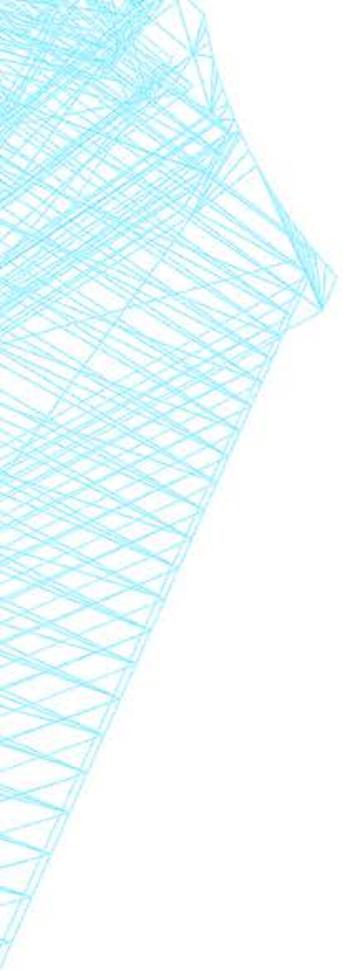
## STRENGTH OF AUTHENTICATION APPROACH (15 POINTS)

Reviewers will evaluate the appropriateness, quality, completeness, and effectiveness of the applicant's proposed approach to leverage a secure and reliable method of authentication.

# SUPPORTS STANDARDS FOR INTEROPERABILITY (5 POINTS)

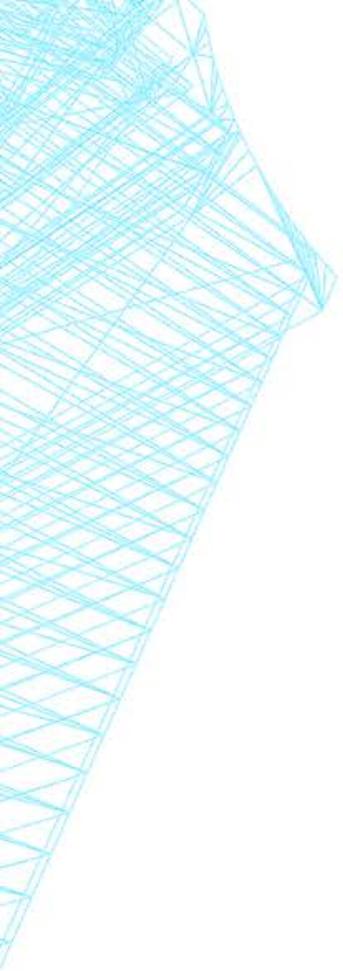
Reviewers will evaluate how well the proposed solution complies with or leverages widely adopted interoperability standards and specifications, as appropriate, such as:

- 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](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>)



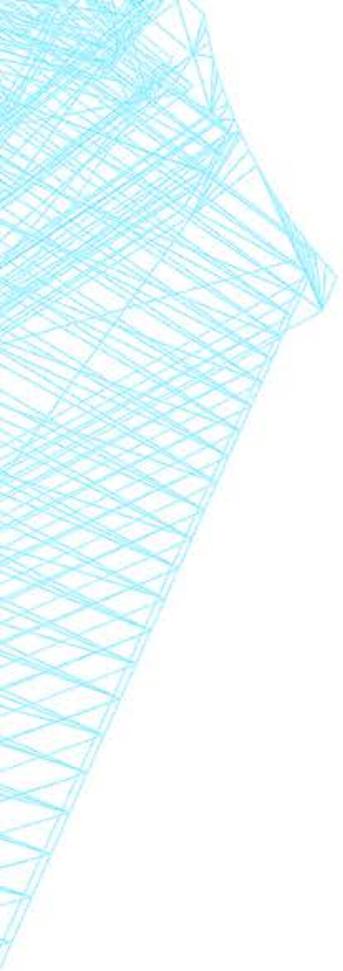
# USABILITY ACROSS TOTAL POPULATION (10 POINTS)

Reviewers will evaluate how well the proposed solution enables disadvantaged or marginalized groups to obtain and use secure online credentials.



# QUALITY OF IMPLEMENTATION PLAN (20 POINTS)

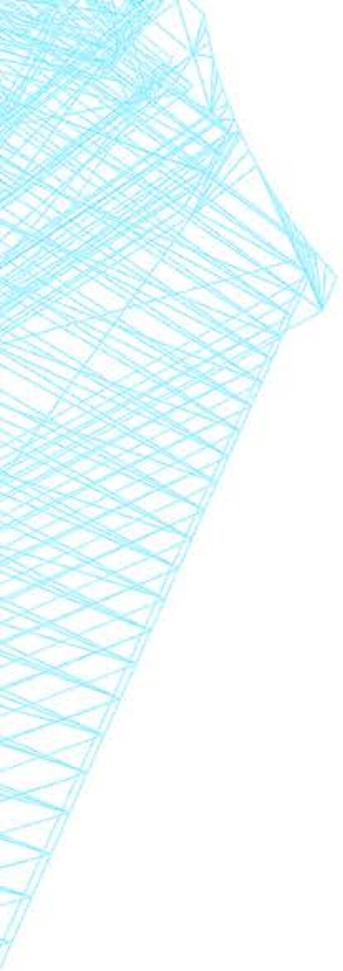
Reviewers will evaluate the appropriateness, quality, completeness and effectiveness of the applicant's plans for implementation including providing an appropriate level of detail on the following: major task descriptions, schedule, quantified objectives, milestones, and measurable metrics that will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



# QUALITY OF IMPLEMENTATION PLAN, CONTINUED

Specifically, reviewers will evaluate the following:

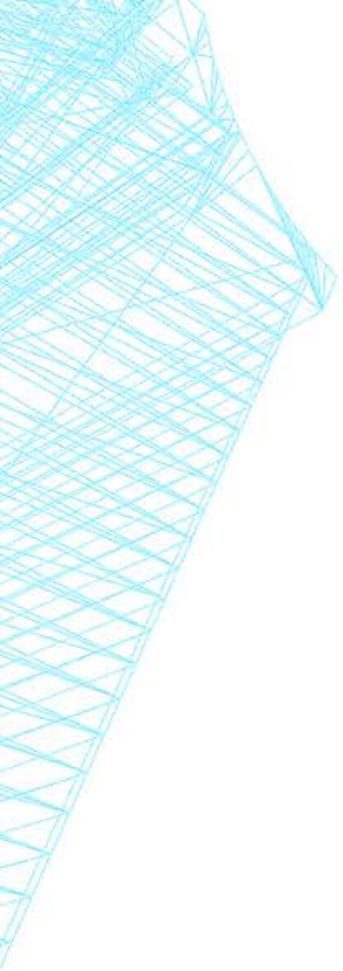
- The completeness of all participants' plans including any required contracting timelines, budget authorizations, and waiver requirements needed;
- How realistic and achievable are the measurable milestones set by the applicant, including metrics encompassing all work on the project including the state programs effected;
- 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; and
- Alignment of the project plan to producing results consistent with the NSTIC Guiding Principles and IDEF requirements.



# IMPACT MEASURES (10 POINTS)

Reviewers will evaluate:

- The uniqueness of the contribution to the Identity Ecosystem;
- The number of potential users in the pilot and the number of potential users if the solution is fully deployed;
- The quality, comprehensiveness, and likelihood of success of the plan to transition a successful pilot into routine use expanding beyond initial pilot users and the award period;
- The potential for impacting the provision of state and local services within the state(s) involved in the pilot;
- The potential for impacting the provision of services states other than the pilot location(s); and
- The quality of described metrics.

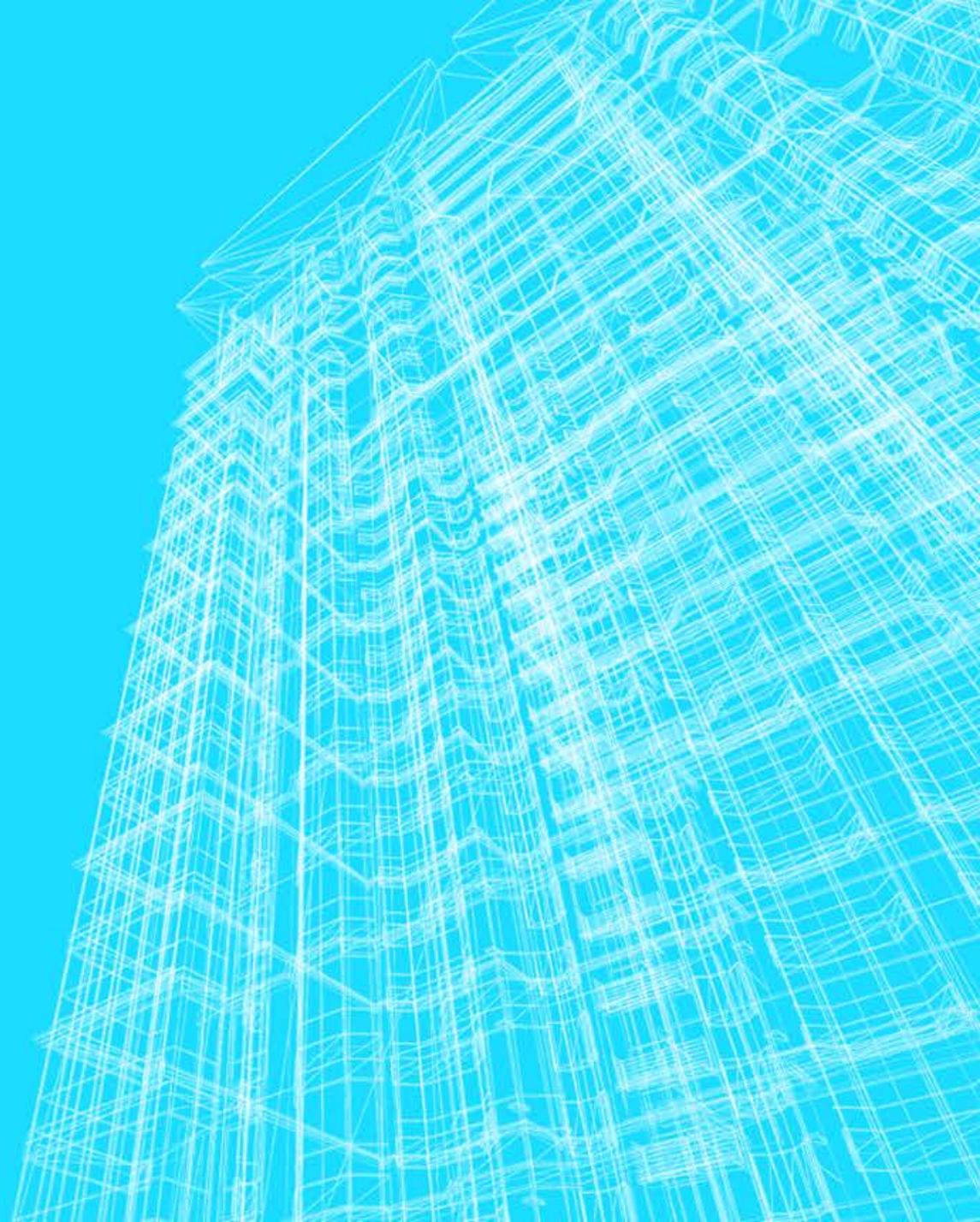


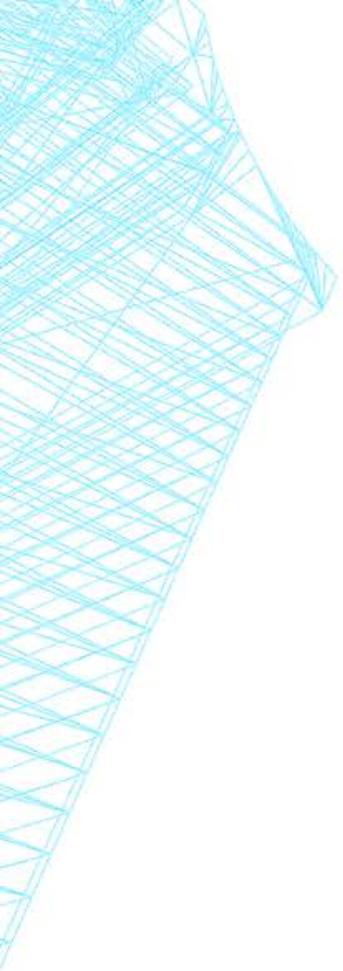
# RESOURCE AVAILABILITY (10 POINTS)

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.

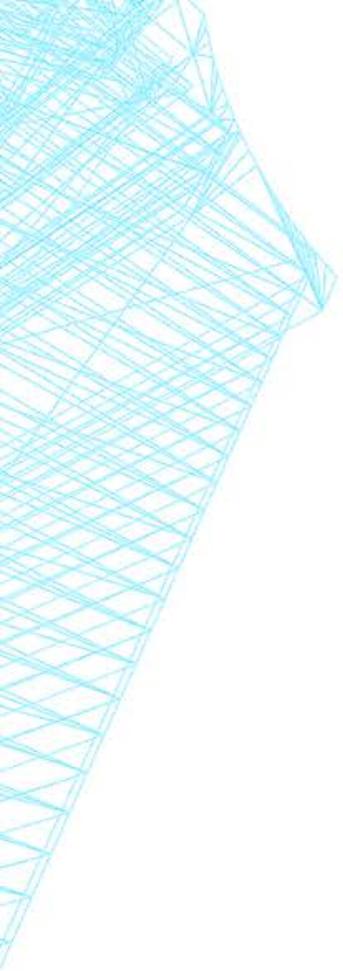
# FUNDING, APPLICATION SUBMISSION AND EVALUATION AND SELECTION PROCESS





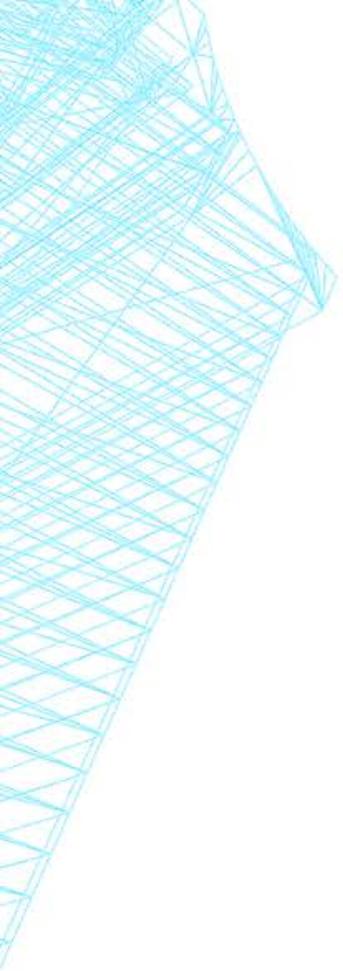
# APPLICATION SUBMISSION

- 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

- Up to \$4 million may be made available in FY 2016
- New awards are expected to range from approximately \$1,000,000 to \$1,250,000 per year each with project performance periods of up to three (3) years
- Initial funding only provided for first year



# FUNDING

## **A note on the ranges:**

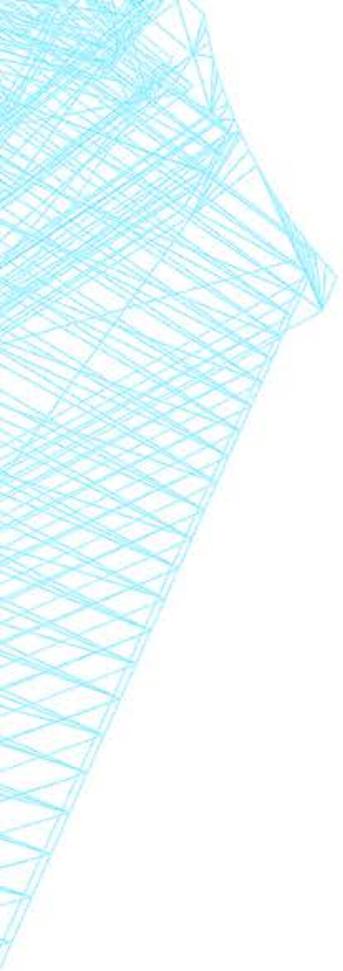
- Applicants may request smaller amounts than the range
- Number of awards will be contingent on available funding
- Three years is the maximum we would consider for a period of performance – entities who can demonstrate meaningful outcomes in a shorter timeframe should propose to do so.

# WHO IS AN ELIGIBLE APPLICANT?

- State, local, and tribal governments
- Accredited institutions of higher education, Non-profit organizations, and Commercial organizations that have at least two state, local, or tribal government agencies representing two different governmental jurisdictions participating in the pilot

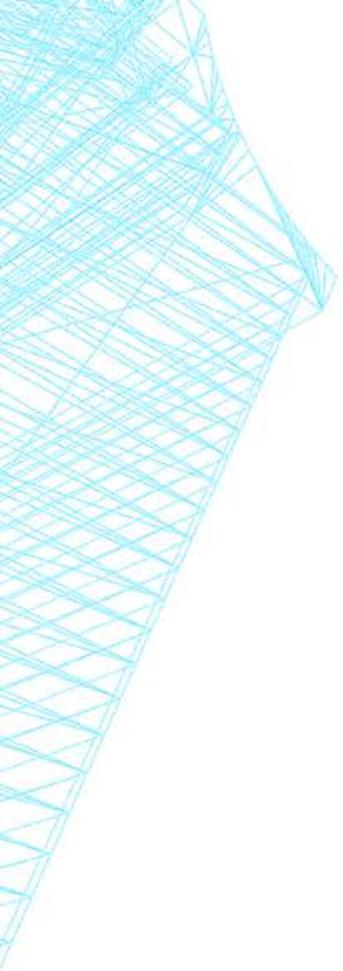


located in the United States and its territories



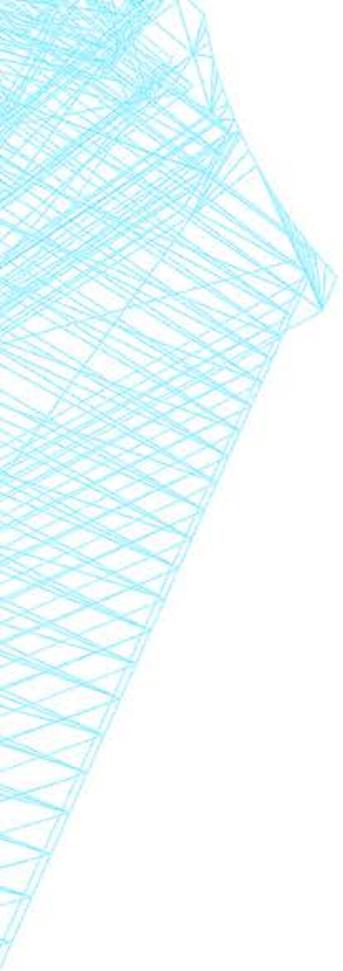
# WHO IS NOT ELIGIBLE TO LEAD A PROJECT?

- Individuals
- Federal government entities may not receive NSTIC funding
- Entities located outside U.S.



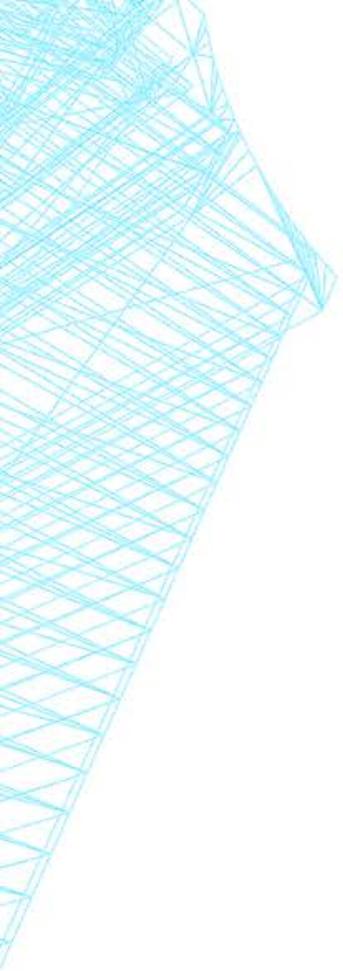
# APPLICATION EVALUATION PROCESS – ABBREVIATED APPLICATIONS

- Administrative Review
  - Eligibility
  - Completeness
  - Responsiveness to the Scope
- Technical Review
  - Evaluation Criteria for Abbreviated Applications
  - At least three independent reviews



# APPLICATION EVALUATION PROCESS – FULL APPLICATIONS

- Administrative Review
  - Eligibility
  - Completeness
  - Responsiveness to the Scope
- Technical Review
  - Evaluation Criteria for Full Applications
  - 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



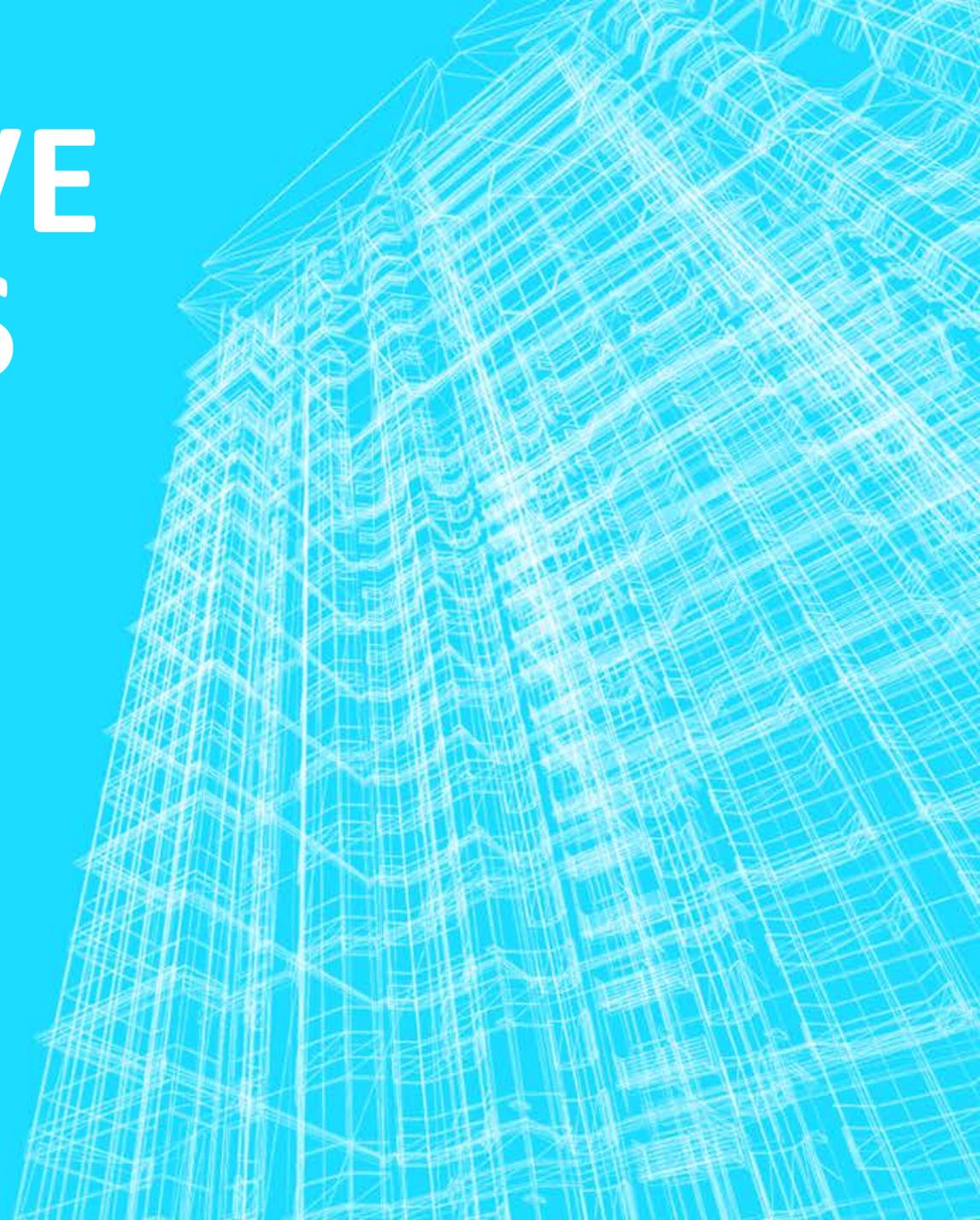
# SELECTION FACTORS

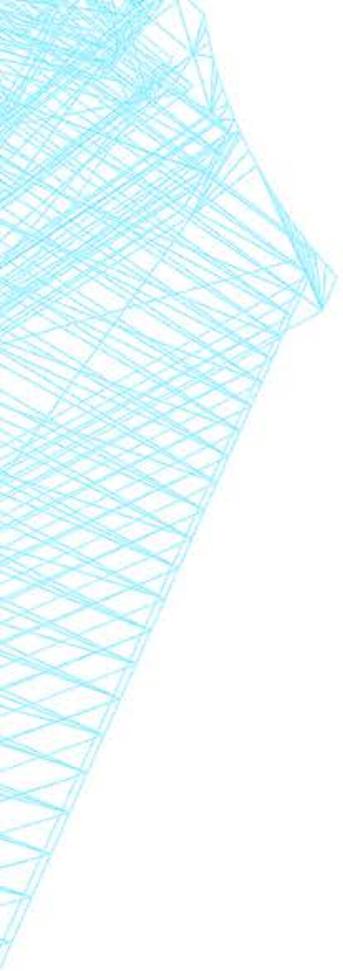
- a.** The availability of Federal funds;
- b.** Whether the project duplicates other projects funded by NIST, DoC, or by other Federal agencies;
- c.** Diversity among the funded projects in state, local and tribal government programs addressed;
- d.** Geographic diversity among the pilots; and
- e.** Diversity of technical approaches across all funded projects to providing a foundation for the Identity Ecosystem.

# ADMINISTRATIVE REQUIREMENTS

**DEAN IWASAKI**

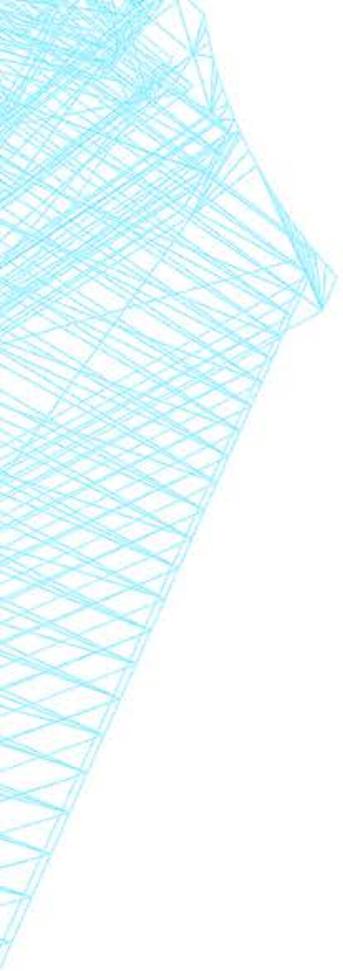
**NIST GRANTS SPECIALIST**





# CONTENTS

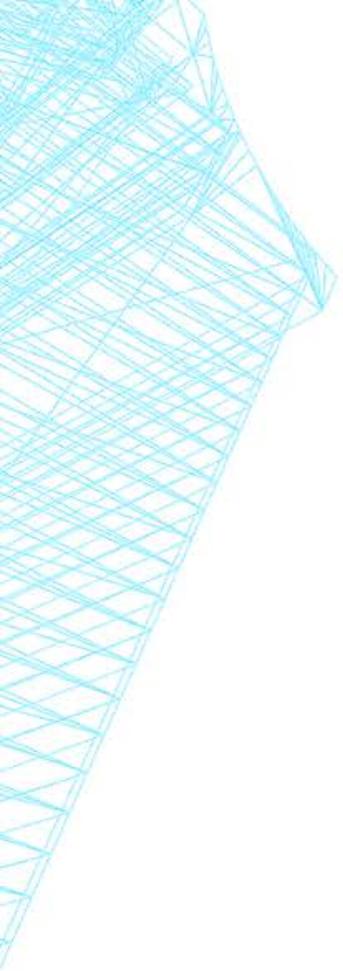
- Budget Narrative Format
- Budget Narrative Content
  - Contracts vs. Subawards
  - Indirect Costs
- Allowable and Unallowable Costs
- Award Requirements
- Payment of Grant Funds
- Reporting Requirements
  - Performance and Financial Reports
  - Intellectual Property



# 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.



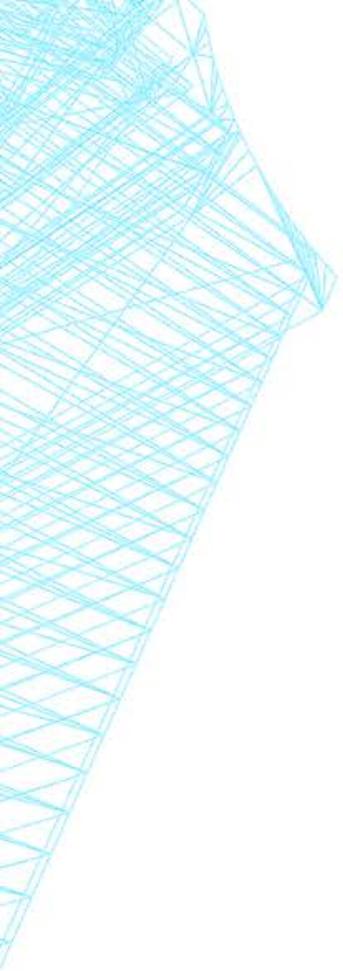
# BUDGET NARRATIVE CONTENT

## 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.



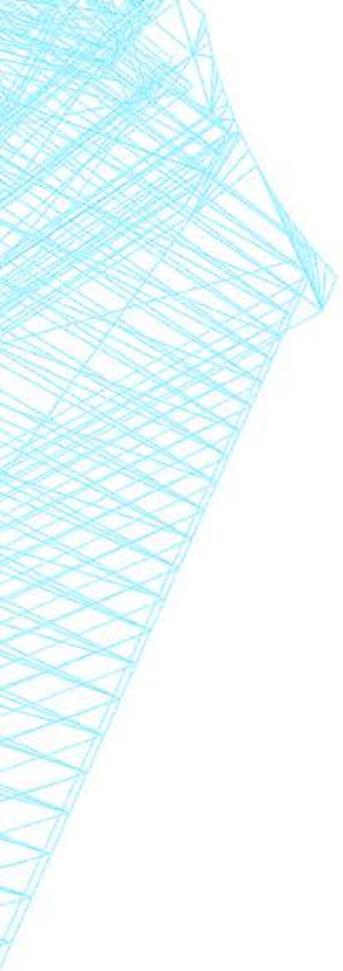
# BUDGET NARRATIVE CONTENT

## **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.



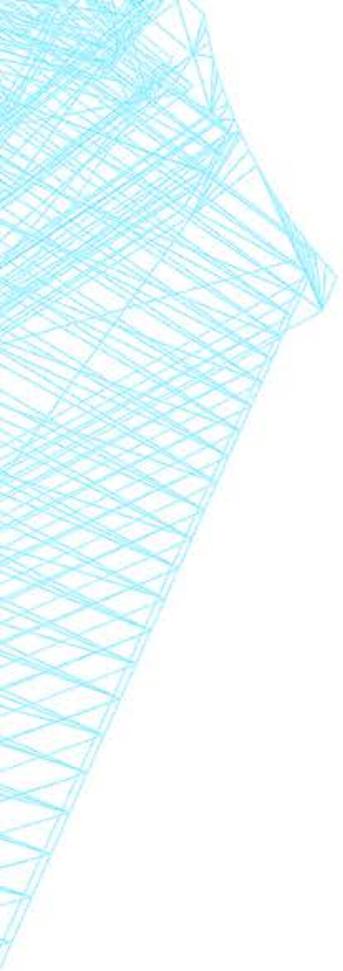
# BUDGET NARRATIVE CONTENT

## 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

### Subaward

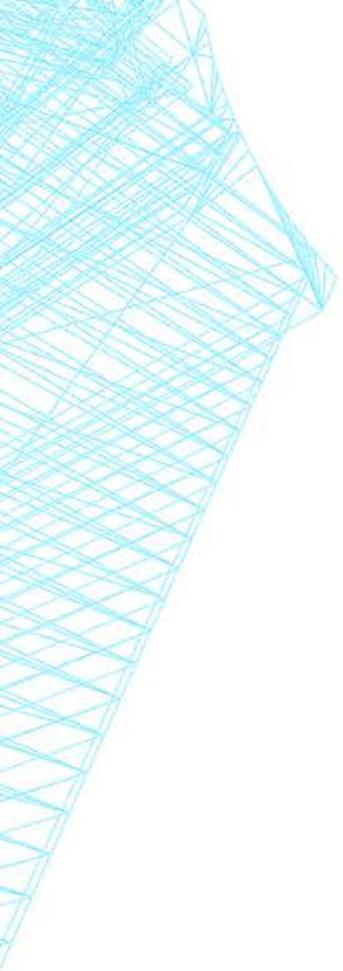
An award of financial assistance made under an award by a recipient to an eligible sub-recipient or by a sub-recipient to a lower tier sub-recipient (DoC Grants Manual).

### 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

### 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).



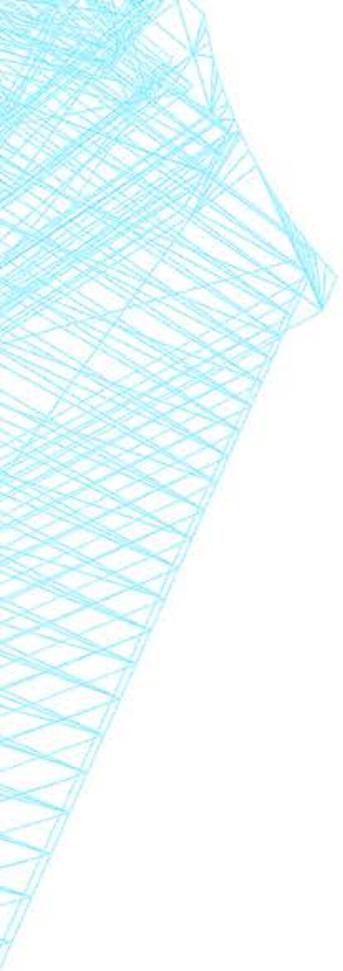
# BUDGET NARRATIVE CONTENT

## **g. Construction**

- Not an allowed cost under this program.

## **h. Other Direct Costs**

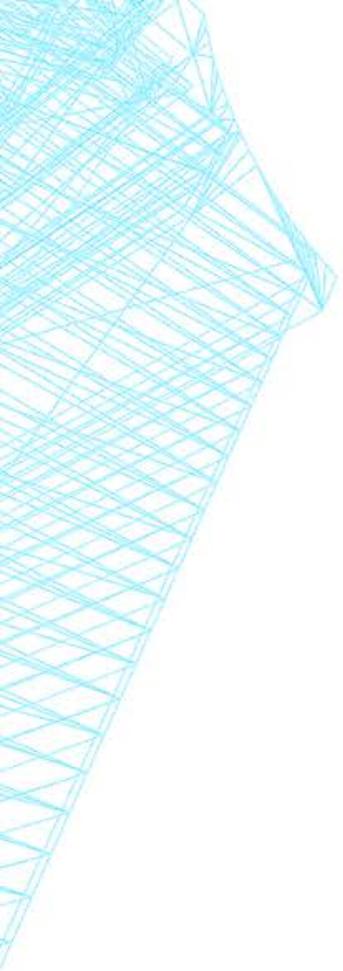
- Costs that do not easily fit into the other cost categories.
- Identify the cost, and provide a breakdown of the cost by quantity or unit of cost.
- Describe the necessity of the cost for the completion of the project.



# BUDGET NARRATIVE CONTENT

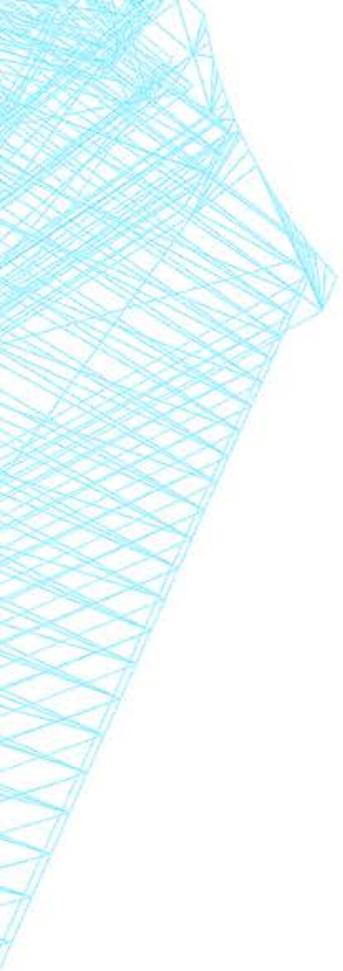
## j. Indirect Charges

- 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](mailto:dean.iwasaki@nist.gov).
  - Use the 10% De Minimis Rate, authorized by 2 CFR 200.414.



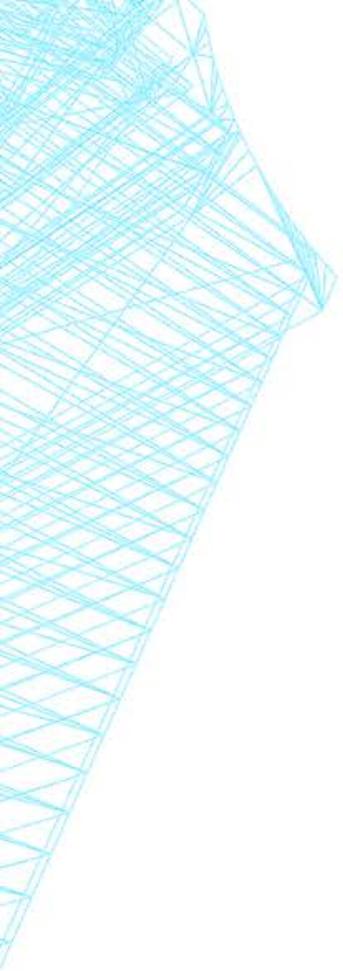
# ALLOWABLE COSTS

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



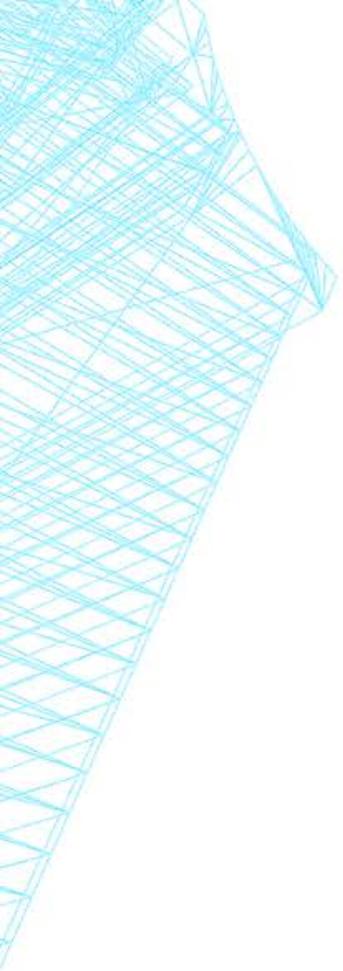
# ALLOWABLE COSTS

- 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.



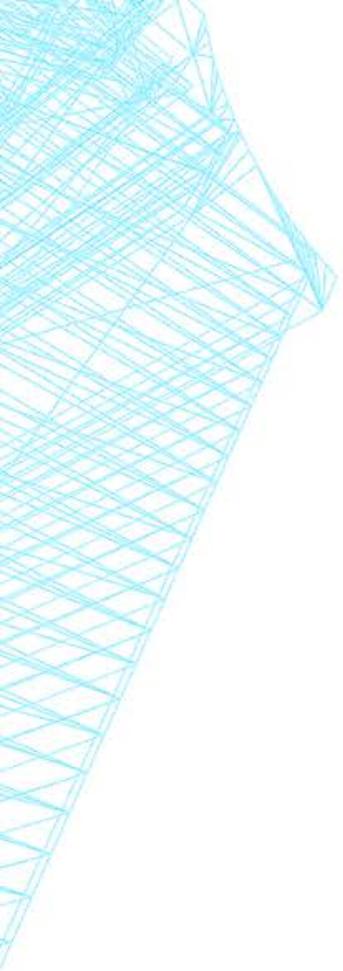
# UNALLOWABLE COSTS

- 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



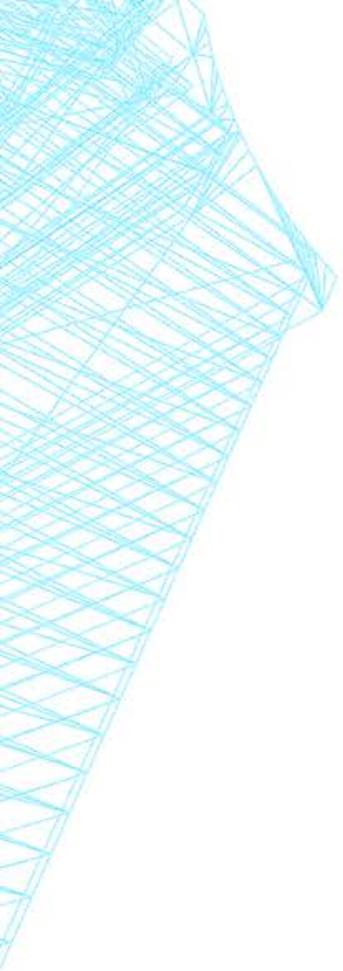
# AWARD REQUIREMENTS

- 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



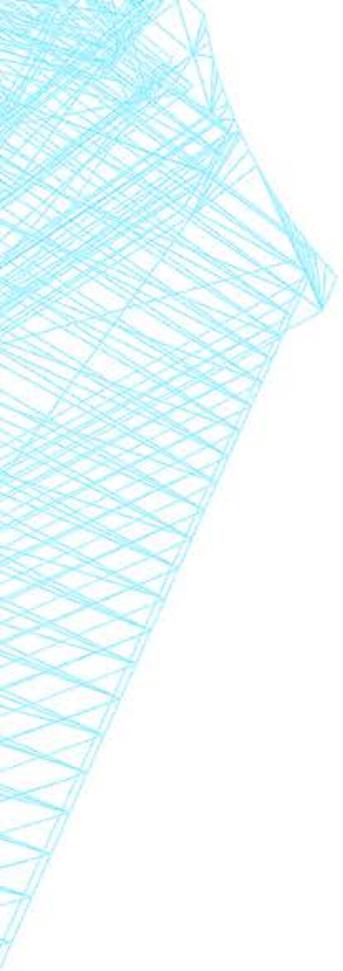
# PAYMENT OF GRANT FUNDS

- 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.



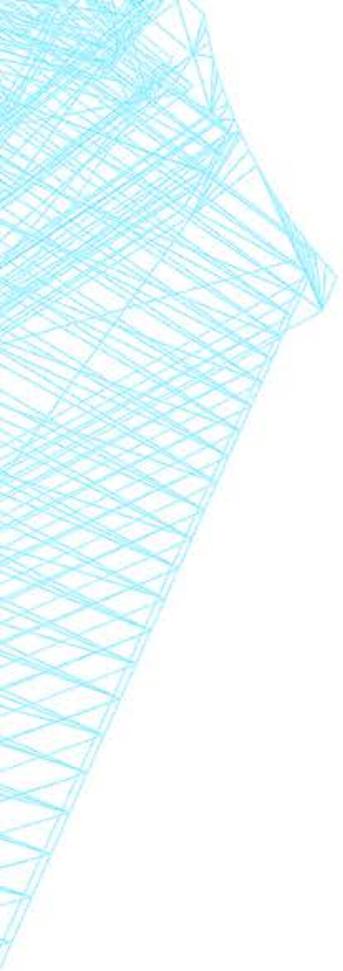
# REPORTING REQUIREMENTS

- **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](https://www.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

