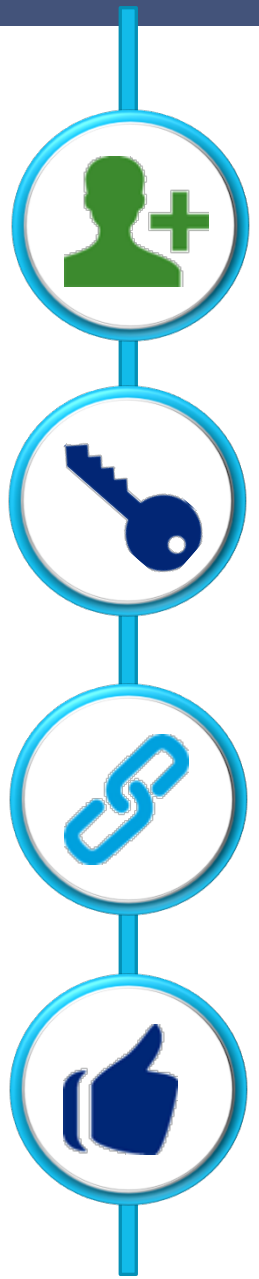


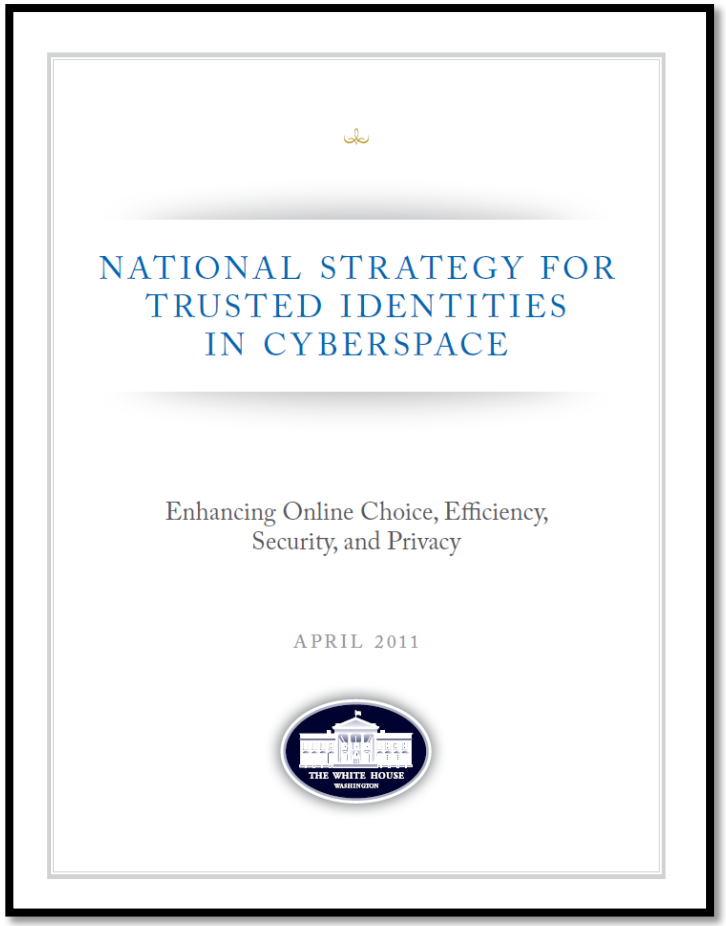
NSTIC at 4: Putting an Ecosystem Into Operation

MIKE GARCIA
DEPUTY DIRECTOR
NSTIC NATIONAL PROGRAM OFFICE, NIST

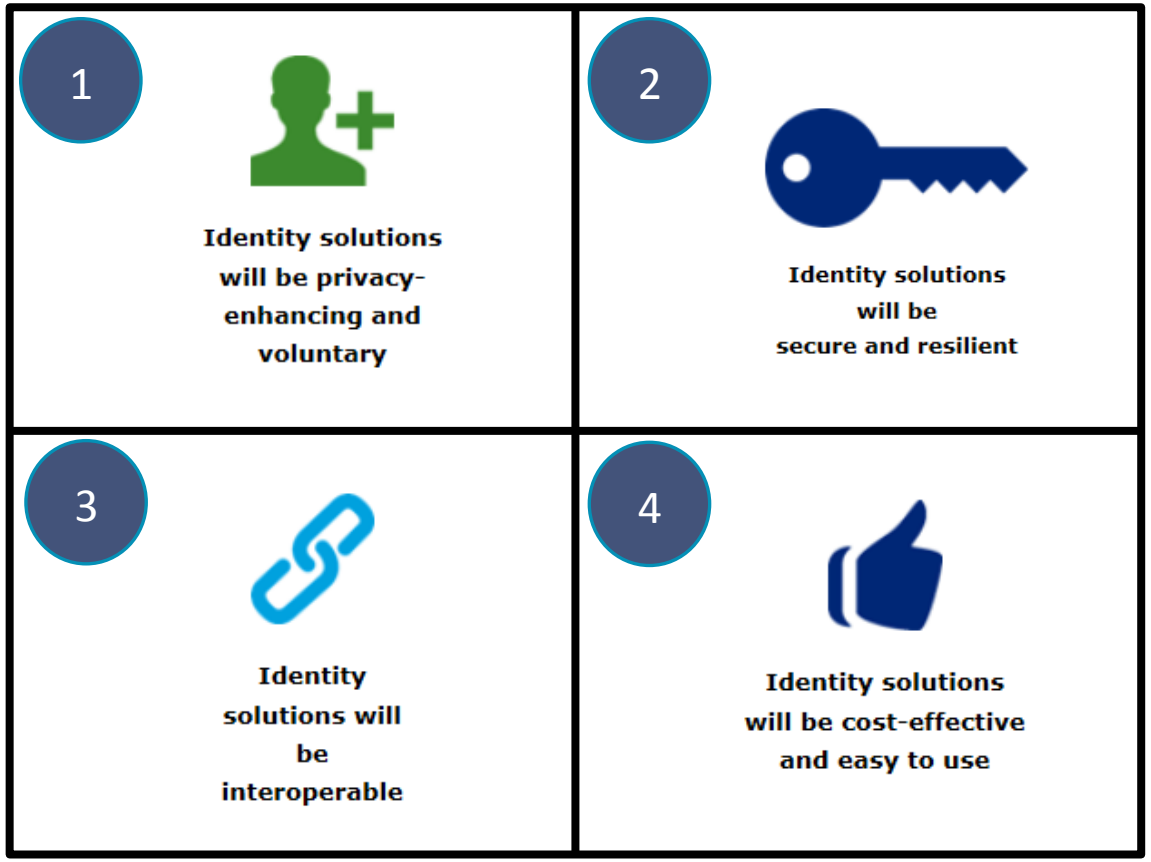
Today's Agenda…

- Very quick NSTIC update
  - No discussion of the problem today—from now on we only talk solutions
- An odd but fitting personal history
- Privacy policy v privacy technology
- A few words about economics
- Tying it all together with a bow

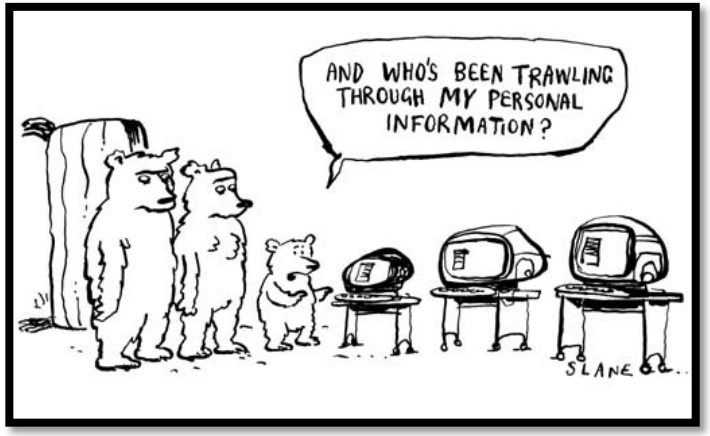
Almost Four Years Ago…



An Identity Ecosystem…with 4 Guiding Principles

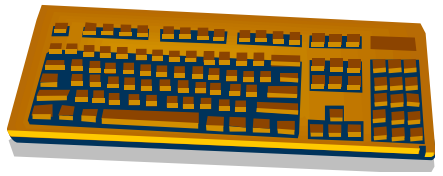


Identity is Central to…



Our Ultimate Goal…

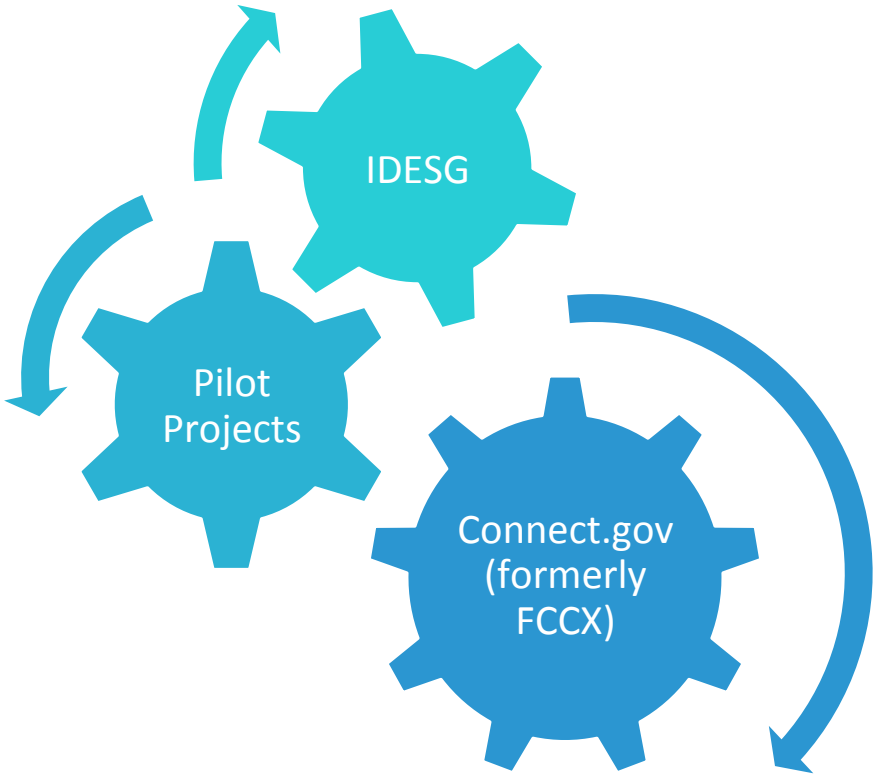
Catalyze the marketplace – so that all Americans* can soon choose from a variety of new types of solutions that they can use in lieu of passwords…



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

* We work toward this goal with everyone in mind—not just Americans—but American taxpayers pay us, so they're number one.

How We're Getting to Our Goal…



Identity Ecosystem Steering Group (IDESG)

- A privately-led group with an increasingly global focus

Pilot Projects:

- Catalyzing a marketplace of solutions and infrastructure

Connect.gov:

- Formerly Federal Cloud Credential Exchange (FCCX or "f-six")

Who is Involved in the IDESG?

- 200+ firms/organizations; 60+ individuals
- Elected Plenary Chair (Kim Sutherland/LexisNexis) and Management Council Chair (Peter Brown); Elected 16 delegates to Management Council
- Member firms include: Verizon, Visa, PayPal, Fidelity, Citigroup, Mass Mutual, IBM, Bank of America, Microsoft, Oracle, 3M, CA, Symantec, Lexis Nexis, Experian, Neiman Marcus, NBC Universal, Aetna, United Health, Intel.
- Also: AARP, ACLU, EPIC, EFF, and more than 65 universities. Participants from 12 countries.

Committees Include:	
Standards	International Coordination
Privacy	Usability
Security	Accreditation
Heath Care	Financial Sector

Targeting the first half of 2015 to release Identity Ecosystem Framework v1

NSTIC Pilots Impact

More than 140 universities are deploying smartphone-based MFA
(Internet2)

Inova Health Systems is enabling 1500 patients to securely obtain their personal health record, leveraging validated attributes from Virginia's DMV **(AAMVA)**

More than 180,000 kids have been authorized by parents – in compliance with COPPA – to access content at websites
(PRIVO)

A Broadridge/Pitney Bowes joint venture has launched targeting 140 million customers for secure digital delivery of financial services content, bill presentment and bill pay
(ID/Dataweb identity solution)

More than 300,000 Veterans can access online services from more than 70 organizations without having to share documents containing sensitive PII to prove Veteran status
(ID.me)

Connect.gov LOA Details

- **LOA 1 & 4:** today (FedRAMP provisional AtO this month); currently Google, Yahoo, Verizon, PayPal, ID.me, PIV/CAC
- **LOA 2 & 3:** within a few months; 2 contracts to commercial credential service providers for USG-wide authentication and attribute validation)

CONNECT.GOV

A personal note on how I got here today…

Access Requirement	Claim	Type	Qualification	3rd	Access
Know how to make a PDF	Knew how to make a PDF	Self	Knew how to make a PDF	None	☑
Know SQL	Knew SQL	Self	Software Engineer	Prev.	☑
Know statistics	Knew stats	Self	Econ grad student	Prev.	☑
Know modeling	Knew modeling	Self	Econ grad student	Prev.	☑
Know the private sector	Sure	Self	Market research manager	Prev.	☑
Know cybersecurity in private sector	Why not	Self	Former navigation control systems coder	Prev.	☑
Know online identity	Have an online identity	Self	Had an online identity	Prev.	☑
Know public private partnerships (PPPs)	Familiar with the term	Self	Vaguely familiar with the term	Prev.	☑
Know standards, contracts, grants budgets, HR, mgmt., crypto, etc.	Is there a pay raise?	Self	No really, how big is the pay raise?	Prev.	☑

Great story…so what?

Notably…

- Only one entity cared about my actual identity: the IRS
- At no point did anyone see anything that isn't fairly easily forged—if they asked for evidence at all
- The entire chain of trust was built on self-assertions and assertions of a 3rd party from the previous step

But it worked because…

- These are temporal interactions; not arms'-length
- There's built-in LOA 1 through human recognition
- We're all very used to face-to-face interactions

Which real world analogs translate online?

1. The internet is the starbucks of physical world transactions.
   - You may think you're having a personalized experience, but in the end you're just another white cup covered in black marker.
2. Online service providers are like—and often run by—aging dads.
   - "I will not throw out that database of personal information! It might be *worth something some day*!"
3. Give a person a phish, she'll buy petrol with your credit card. Teach a person to phish, she'll steal 1.2 billion passwords.
   - No matter how good your policy, bad technologies will fail

And what do these analogs imply?

1. Online service providers are somewhere between curio salesperson at Sacre Coeur and hot dog guy outside your building.
   - If you really need something you'll go get it, but you'd rather send your assistant—or your grad student, as the case may be.
2. You don't ask a hoarder to stop, you have to disempower him.
   - If you want better privacy online, don't think SPs will do it for you. Move them to a small apartment and stop taking them to garage sales.
3. Bad actors will find ways as long as you keep the pond stocked.
   - The sustainable answer is to continuously devise new technological means to limit the utility of personal information, not just secure it.

Privacy policy enforced by privacy technology

- We must believe in the old adage:

  Fool me once, shame on you

  Fool me with a 5,000-word privacy policy, shame on me

- Good polies are good to have, but good technologies are superior
- It doesn't matter what your privacy policy is, the important thing is that your technology supports it
- That takes away the burden (and excuse) of being hard to do the right thing
- Indeed, it frees you to do the right thing

Is privacy turning out just how people want it?

- People too often use economics to support the status quo.
  - If the market were already offering what consumers wanted, we wouldn't need innovation…consumers face **limited option sets**
  - Consumers participate in constrained optimization. They work to improve utility, not perfect it.
- There are **high search costs** associated with a consumer managing her personal information
  - Carnegie Mellon study: 76 workdays to read all privacy policies
  - Add to this costs of maintaining privacy settings—on each site, remediating when problems occur, and on and on

Don't people change when they're unhappy?

- With **high switching costs**, it can be too costly for a consumer to switch to a competitor, so he keeps an inferior service
  - Switching email providers, social media networks, etc., can cause costs through learning curves, loss of social connectivity
  - In competitive theory, substitutions must be frictionless. A cursory glance shows they're not.
- **Background risk**—whether latent or salient—can influence foreground decision making
  - If an individual thinks protecting her privacy is already a lost cause, there's no reason to put any effort into protecting it at the next service provider

What does this all add up to?

- I'm talking to you because of the attributes I have, not who I am
  - Whenever possible, this should be axiomatic in online transactions
- Coming up with better policies is a great idea. Coming up with easier ways to implement those policies is even better.
  - The NSTIC approach is holistic, but we favor technology solutions built to work over policy solutions written to work.
- Nothing can elude the economics for long
  - Individual orgs don't tend to solve hairy economic problems. Find solution sets collaboratively, then innovate solutions competitively

Questions?

Michael Garcia, Ph.D.
Deputy Director, NSTIC
National Institute of Standards and Technology
U.S. Department of Commerce
www.nstic.gov
michael.garcia@nist.gov

Identity Ecosystem Steering Group
www.idecosytem.org

Check our Funding Opportunities page: http://www.nist.gov/nstic/funding-opportunities.html