



NSTIC at 4: Putting an Ecosystem Into Operation



After 21 years, we still can't solve this



"On the Internet, nobody knows you're a dog."

76%

NETWORK INTRUSIONS
EXPLOITED **WEAK** OR
STOLEN CREDENTIALS



46%

OF CONSUMERS
WILL ABANDON A
SITE RATHER THAN
ATTEMPT TO
RESET THEIR
PASSWORDS OR
ANSWER SECURITY
QUESTIONS



25

...IS THE AVERAGE
NUMBER OF
ACCOUNTS A USER
HAS THAT
REQUIRE
PASSWORDS

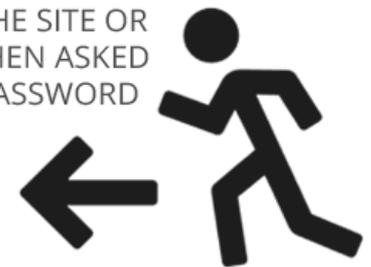


6.5

...IS THE AVERAGE
NUMBER OF
WEB PASSWORDS
HELD BY A USER

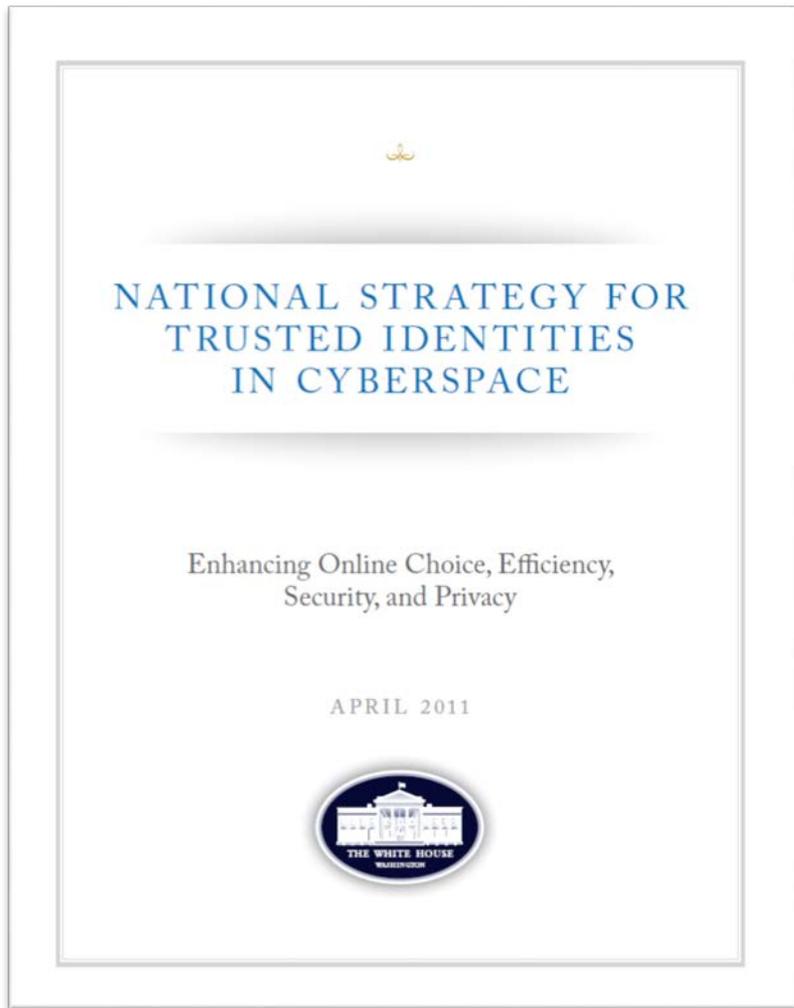
54%

...OF USERS LEAVE THE SITE OR
DO NOT RETURN WHEN ASKED
TO CREATE A NEW PASSWORD





Three Years, Eleven Months, and Eight Days Ago...



An Identity Ecosystem...with 4 Guiding Principles



Identity solutions will be privacy-enhancing and voluntary



Identity solutions will be secure and resilient



Identity solutions will be interoperable



Identity solutions will be cost-effective and easy to use

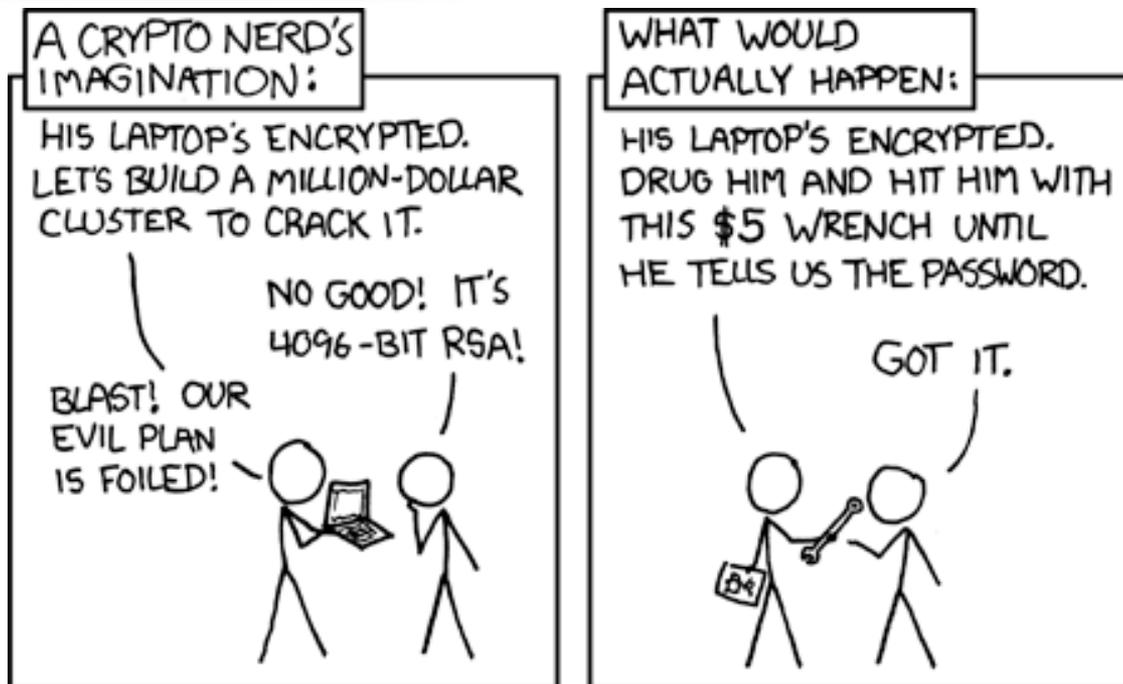


Why NSTIC?

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



It's not all about security



Source: *xkcd*

Usability

Privacy

Interoperability

Liability

Business Models

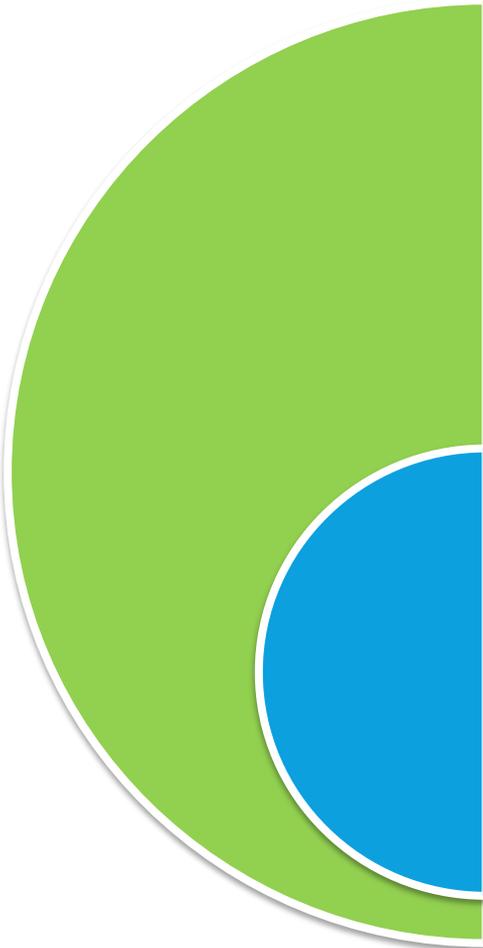


Why NSTIC?

- 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 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.**



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
- Leadership includes Citi, Lexis-Nexis, Symantec, Salesforce, Oracle, Aetna, US Bank and Neiman Marcus – as well as AARP, Patient Privacy Rights, and other advocates.

Fund Innovative Pilots to Advance the Ecosystem

- 4 rounds of pilot grants since 2012, 5th round expected in September
- 15 pilots funded in total; 11 now active

Government as an early adopter to stimulate demand

- White House effort to create **Connect.gov**, a single service for identity at public facing government applications.
- October 2015: **Executive Order 13681**, requiring all USG digital applications that release personal data to require Multi Factor Authentication (MFA) + an effective identity proofing process



CONNECT.GOV

Enabling trusted digital interactions between people and government

NIST

GSA

 **UNITED STATES
POSTAL SERVICE**



Vision and Mission



VISION

Enabling trusted digital interactions between people and government.



MISSION

Connect.Gov enables people to access digital government services in a convenient, privacy enhancing, and secure manner without having to necessarily create a new login.



Connect.Gov Background

CONNECT.GOV IS CURRENTLY IN ITS FIRST PHASE OF OPERATIONS

September 2009:

The Identity, Credential, and Access Management Subcommittee (ICAMSC) released the Trust Framework Provider Adoption Process.

March 2012:

The Federal Cloud Credential Exchange (FCCX) tiger team convened to define a common cloud-based service.

October 2014:

Executive Order – Improving the Security of Consumer Financial Transactions was released.

October 2011:

OMB released a memo – Requirements for Accepting Externally Issued Identity.

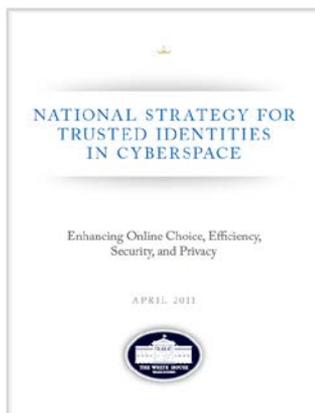
December 2013:

National Strategy for Information Sharing and Safeguarding was released.





Connect.Gov Drivers



National Strategy For Trusted Identities In Cyberspace (NSTIC)



Executive Order – Improving The Security of Consumer Financial Transactions

“...ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.

Within 18 months of the date of this order, relevant agencies shall complete any required implementation steps set forth in the plan prepared pursuant to this section.” – Executive Order, Improving the Security of Consumer Financial Transactions



Federated Identity for the Federal Government

Authenticate User's Identity Once – Re-use Across Government

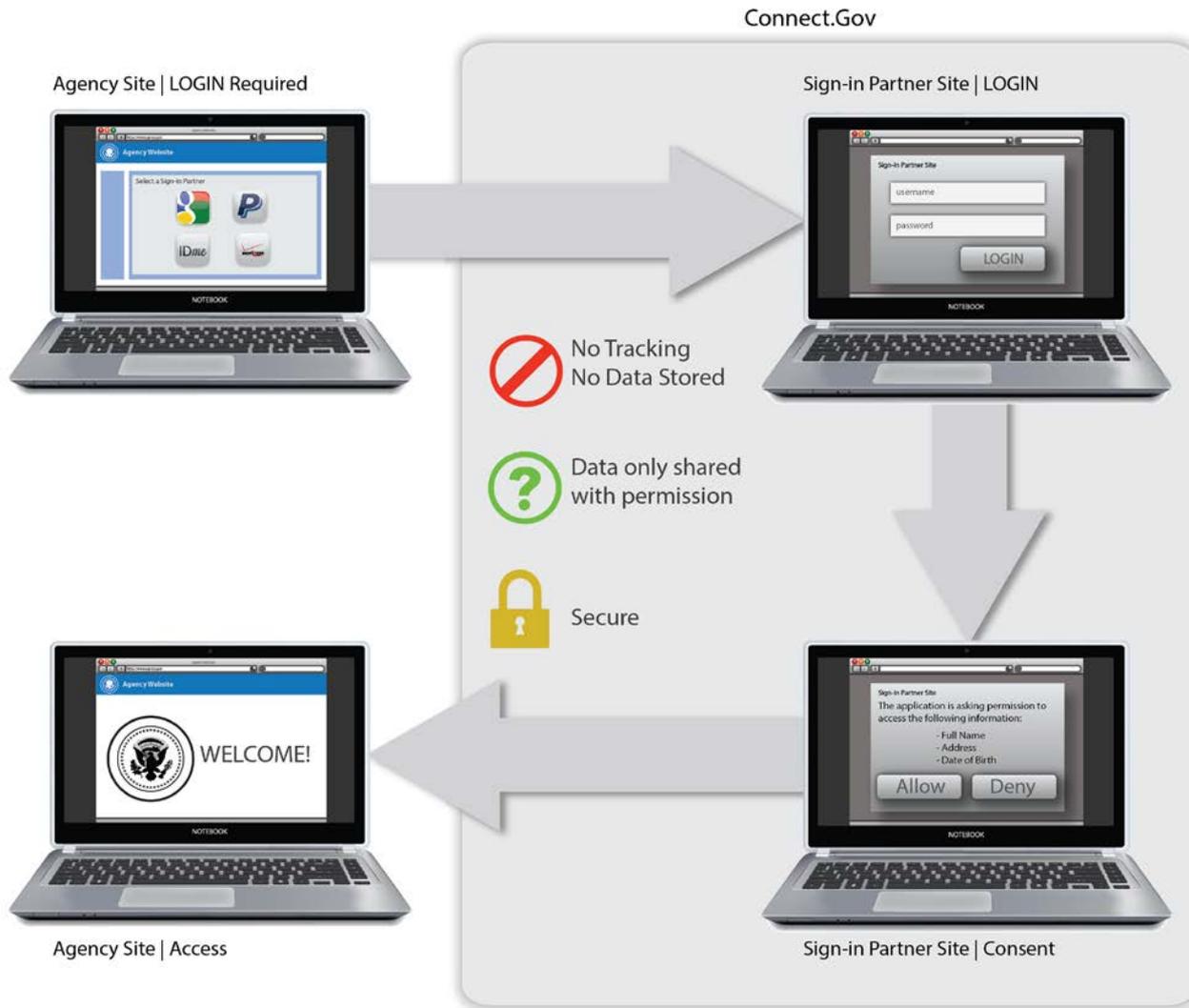


Levels of Assurance

Connect.gov provides enhanced security and privacy services and has the capability to accept digital credentials at Level of Assurance (LOA) 1, 2, 3 and 4.

Level of Assurance		LOA 4 – Very High Confidence in Asserted Identity
		LOA 3 – High Confidence in Asserted Identity ✦
		LOA 2 – Some Confidence in Asserted Identity
		LOA 1 – Little or No Confidence in Asserted Identity

✦ *Greatest need for citizen identity proofing and authentication*



Agency Benefits



INCREASES SECURITY & PRIVACY

Facilitates strong authentication of users that need access to an agency's online services, while protecting their privacy and personal data.



STREAMLINES ACCESS

Provides an agency with a "one stop shop" for authenticating users to online applications, reducing the need to provision and manage multiple credentials and user identities across the organization.



ENABLES DIGITAL SERVICES

Offers credentials with a high level of trust to allow more personalized information and applications to be delivered online.



REDUCES INVESTMENT

Enables the re-use of interoperable credentials across agencies, provides multi-factor authentication, and eliminates the need for an agency to provision and manage credentials.



Consumer Benefits



SIMPLIFIES ACCESS

Allows use of a single government approved credential to interact with multiple agencies and applications.



PROTECTS PRIVACY

Consumers control decision to share their identity and personal data and solution prevents tracking of consumers' online government activities.



ENHANCES USER EXPERIENCE

Provides users choice of credentials, streamlines access, and provides a simple consistent way to access government services.



Initial Relying Parties



Veterans Affairs
MyHealthVet



General Services Admin.
Federal Real Property
Program



**Department of
State**
FAN.Gov



**National Institute of
Standards and Technology**
NOTifyUS



**United States Department of
Agriculture**
Ag E-auth



Connect.Gov Website

More information regarding Connect.Gov can be found on our website,
www.connect.gov

CONNECT.GOV

Enabling trusted digital interactions between
people and government



CONTACTS



PROGRAM MANAGEMENT OFFICE



Jennifer Kerber
Jennifer.kerber@gsa.gov



Jonathan Prisby
Jonathan.prisby@gsa.gov

TECHNOLOGY MANAGEMENT



Angela Lagneaux
angela.m.lagneaux@usps.gov