

# National Strategy for Trusted Identities in Cyberspace

---

**James B. Sheire**

**Senior Advisor, NSTIC**

**National Institute of Standards and Technology (NIST)**

**August 26, 2013**



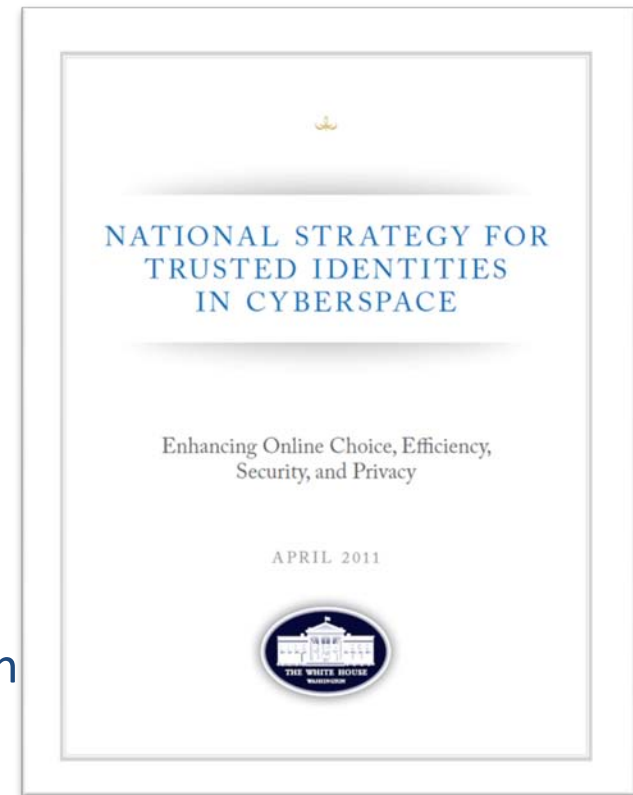
# What is NSTIC?

Called for in President's Cyberspace Policy Review (May 2009):  
a "cybersecurity focused identity management vision and strategy...that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation."

## Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**,  
"an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."



# Problems Today

---

## Username and passwords are broken

- Most people have 25 different passwords, or use the same one over and over
- Even strong passwords are vulnerable...criminals have many paths to easily capture “keys to the kingdom”
- Rising costs of identity theft
  - **11.6M** U.S. victims (+13% YoY) in 2011 at a cost of **\$37 billion**
  - **67% increase** in # of Americans impacted by **data breaches in 2011**  
(Source: Javelin Strategy & Research)
- A common vector of attack
  - Sony Playstation, Zappos, Lulzsec, LinkedIn, among dozens of 2011-12 breaches tied to passwords.

# Problems Today

---

## Password change and New Account Setup are alienating customers

- Many sometimes think it would be easier to solve world peace than attempt to remember all their passwords
- Most would rather undertake household chores, like cleaning the toilet or doing the dishes, than have to create another username and password
- 84% of people dislike being asked to register on a website
- Shopping cart abandonment: 38% online users do not buy online because they have to register before purchasing. (source: Forrester)



# Problems Today

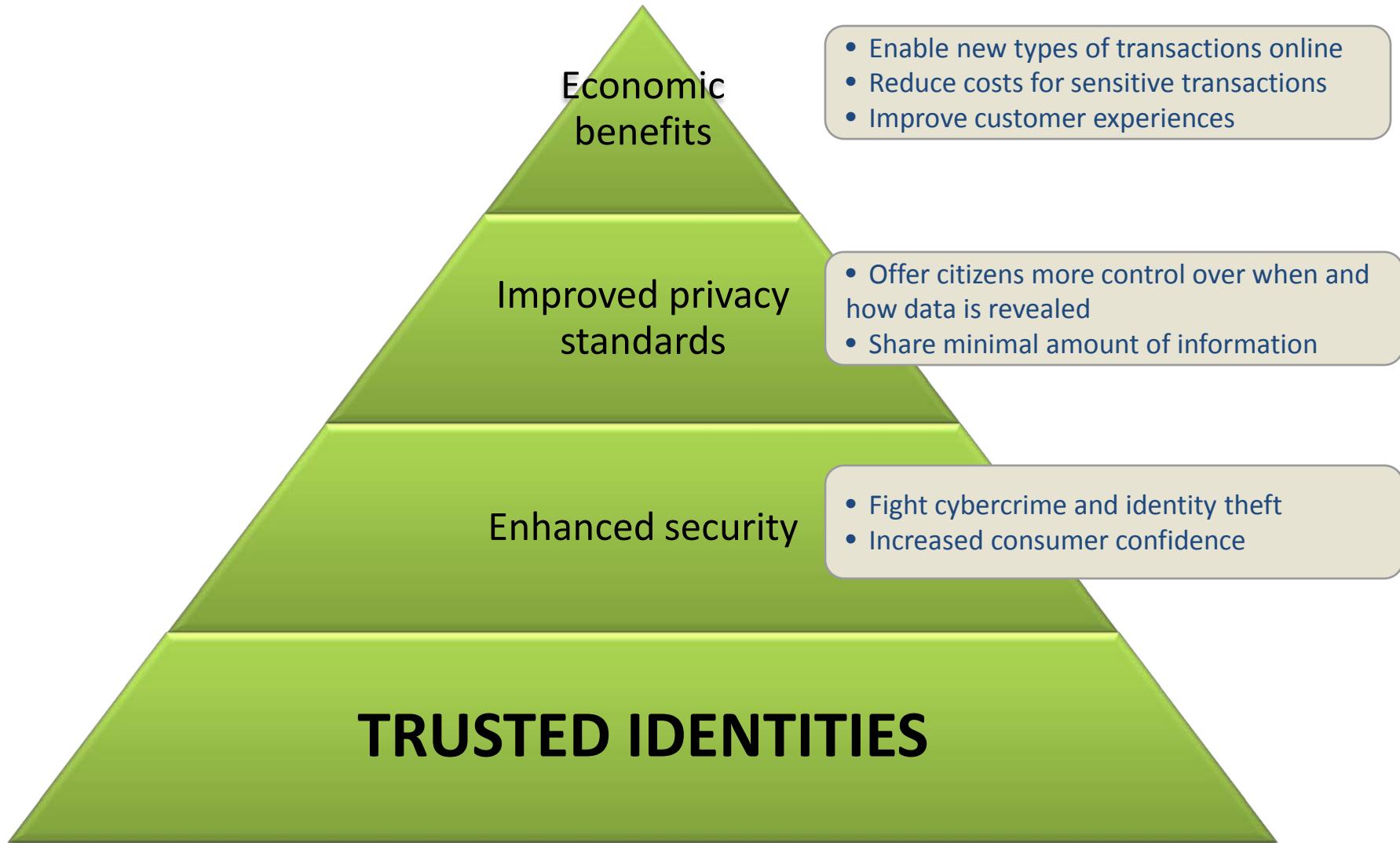
---

## Identities are difficult to verify over the internet

- Numerous government services still must be conducted in person or by mail, leading to continual rising costs for state, local and federal governments
- Electronic health records could save billions, but can't move forward without solving authentication challenge for providers and individuals
- Many transactions, such as signing an auto loan or a mortgage, are still considered too risky to conduct online due to liability risks

# Trusted Identities provide a foundation

---



# January 1, 2016

The Identity Ecosystem: Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime.



Apply for mortgage online with e-signature



Online shopping with minimal sharing of PII

Trustworthy critical service delivery



Secure Sign-On to state website

Security 'built-into' system to reduce user error



Privately post location to her friends



# 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 framework around liability and privacy
- Fund pilots to stimulate the marketplace
- Act as an early adopter to stimulate demand



# Key Implementation Steps

## Convene the Private Sector

- Created an **Identity Ecosystem Steering Group (IDESG)**: Summer 2012  
<http://www.idecosystem.org/>
- NIST awarded 2-year grant to fund a privately-led Steering Group to convene stakeholders and craft standards and policies to create an **Identity Ecosystem Framework**

## Continued Support for Pilots

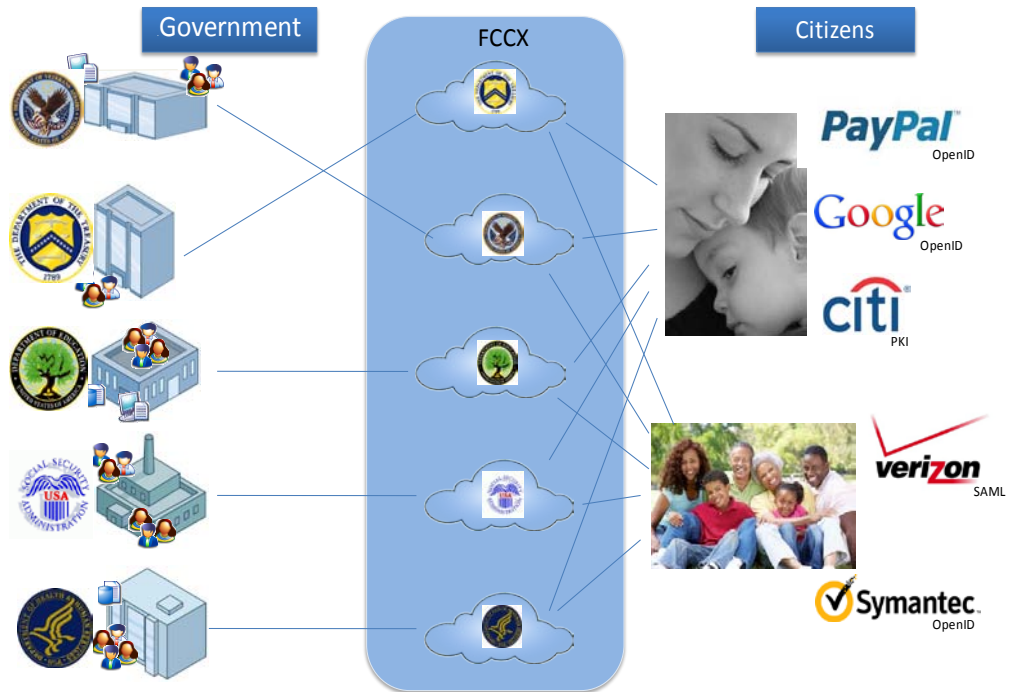
- **5 pilots totaling \$9.2M** awarded September, 2012
- Challenge-based approach focused on addressing barriers the marketplace has not yet overcome
- New pilot grant round for 2013 underway, including new state government FFO

## Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap
- New White House initiated effort to create a **Federal Cloud Credential Exchange (FCCX)**, award to SecureKey announced last week

# The Federal Cloud Credential Exchange (FCCX)

The FCCX will be an enterprise, cloud-based service that can provide all Federal agencies with an ability to accept the full range of FICAM-approved, non-federal government issued, credentials for online services for citizens



# The Identity Ecosystem Steering Group (IDESG)

---

- Provides an open process for organizations to participate in the ongoing coordination, acceleration, harmonization and development of the Identity Ecosystem Framework
- Working Groups developing the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem
- Numerous states participating; management council includes a representative specifically for state and local governments
- Website with registration information: [www.idecosystem.org](http://www.idecosystem.org)
- Next Plenary meeting set for October 16-18 in Washington, D.C. area

# NSTIC Pilots

---

- NSTIC pilots seek to catalyze a marketplace of online identity solutions
- Using privacy-enhancing architectures in real-world environments, the NSTIC pilots are testing new methods for identification online for consumers that increase usability, security, and interoperability to safeguard online transactions
- 2013 round of pilots will include grants focusing on state government use cases

# The AAMVA Pilot

---

- The **Cross Sector Digital Identity Initiative (CSDII)**, led by **The American Association of Motor Vehicles (AAMVA)** is developing technology that will demonstrate the acceptance of commercial identity provider credentials by Virginia state government, including securely verifying identities online with the **Virginia Department of Motor Vehicles**
- State governments, including Virginia, are exploring leveraging commercial identity providers for secure online access to state government websites as a means to improve customer service and reduce the costs associated with online identity management
- In addition to enabling state government services, CSDII is partner with private sector relying parties - newest participant in the AAMVA pilot is **Inova**, a leading Virginia healthcare system
- The CSDII team will provide more detail...

# For More Information

---

James Sheire

[James.sheire@nist.gov](mailto:James.sheire@nist.gov)

Washington, D.C.

+1 202.482.1963



Twitter: @NSTICNPO, #NSTIC



Blog: NSTIC Notes, <http://nstic.blogs.govdelivery.com/>