

# National Strategy for Trusted Identities in Cyberspace

## *Pilots, Policy and Progress*

---



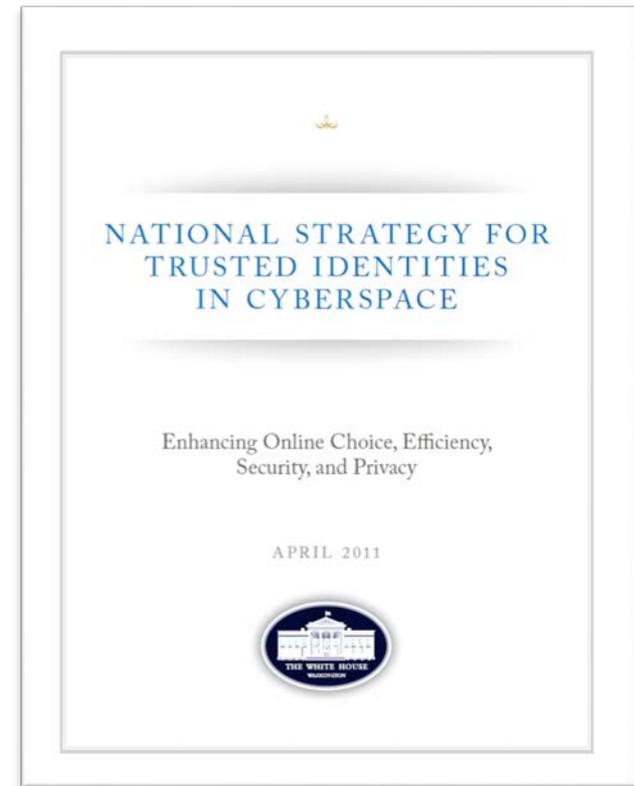
# What is NSTIC?

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."



# Setting the Stage



2004: "The Password is Dead"



2013: "The Password is Dead"

# But – the password is very much alive

## How do breaches occur?

52%

used some form of hacking (-)

76%

of network intrusions exploited weak or stolen credentials (-)

40%

incorporated malware (-)

35%

involved physical attacks (+)

29%

leveraged social tactics (+)

13%

resulted from privilege misuse and abuse

The one-two combo of hacking and malware struck less often this round, but definitely isn't down for the count. Filtering out the large number of physical ATM skimming incidents shows exploitation of weak and stolen credentials still standing in the ring.

The proportion of breaches incorporating social tactics like phishing was four times higher in 2012. Credit the rise of this challenger to its widespread use in targeted espionage campaigns.

Correlated with the 14% of breaches tied to insiders, privilege misuse weighs in at 13%. Insider actions ranged from simple card skimming to far more complicated plots to smuggle corporate IP to competitors.

Source: 2013 Data Breach Investigations Report, Verizon and US Secret Service

# And Passwords Are Killing Us

Table 7. Top 10 Threat Action Types by number of breaches and records

Rank	Variety	Category	Breaches	Records
1	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	48%	35%
2	Exploitation of default or guessable credentials	Hacking	44%	1%
3	Use of stolen login credentials	Hacking	32%	82%
4	Send data to external site/entity	Malware	30%	<1%
5	Brute force and dictionary attacks	Hacking	23%	<1%
6	Backdoor (allows remote access/control)	Malware	20%	49%
7	Exploitation of backdoor or command and control channel	Hacking	20%	49%
8	Disable or interfere with security controls	Malware	18%	<1%
9	Tampering	Physical	10%	<1%
10	Exploitation of insufficient authentication (e.g., no login required)	Hacking	5%	<1%

2011: **5 of the top 6** attack vectors are tied to passwords

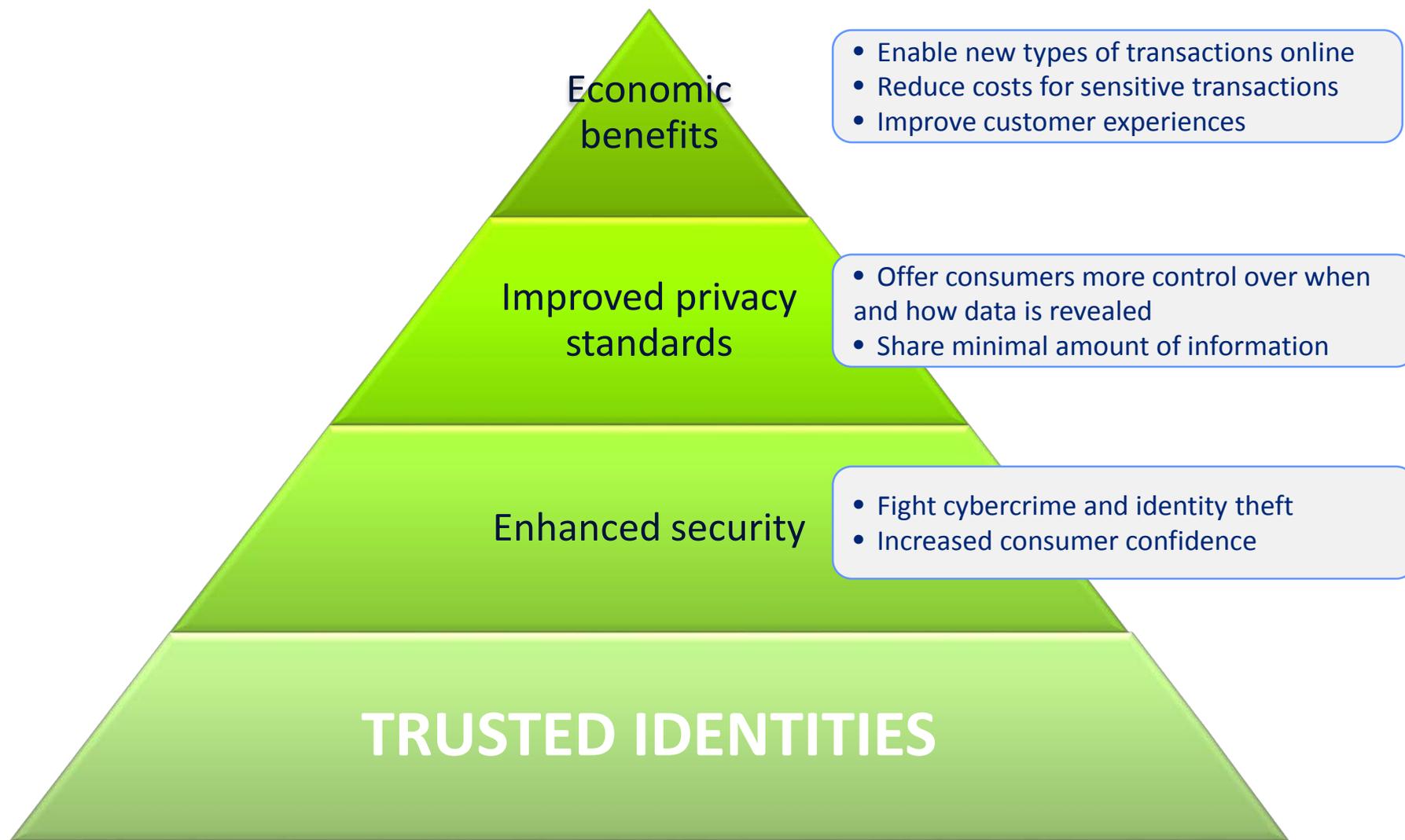
2010: **4 of the top 10**

# Privacy is a growing challenge

- Individuals often must provide more personally identifiable information (PII) than necessary for a particular transaction
- This data is often stored, creating “honey pots” of information for cybercriminals to pursue -- creating potential liabilities for organizations
- Individuals have few practical means to control use of their information



# Trusted Identities provide a foundation

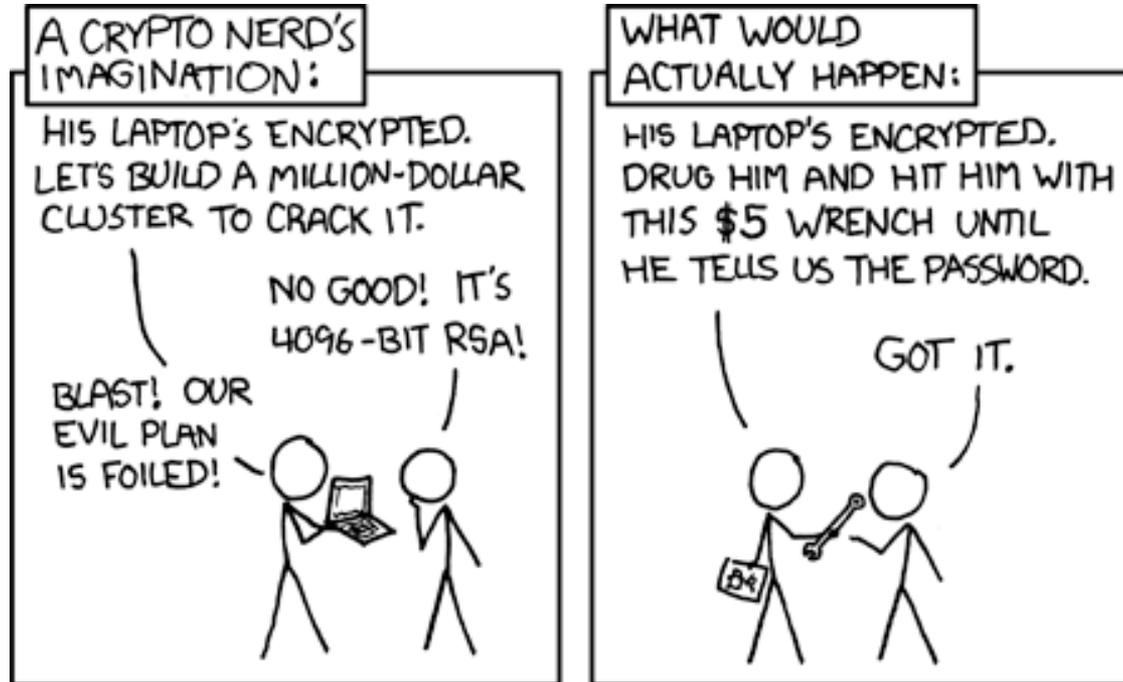


# Why NSTIC?

---

**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

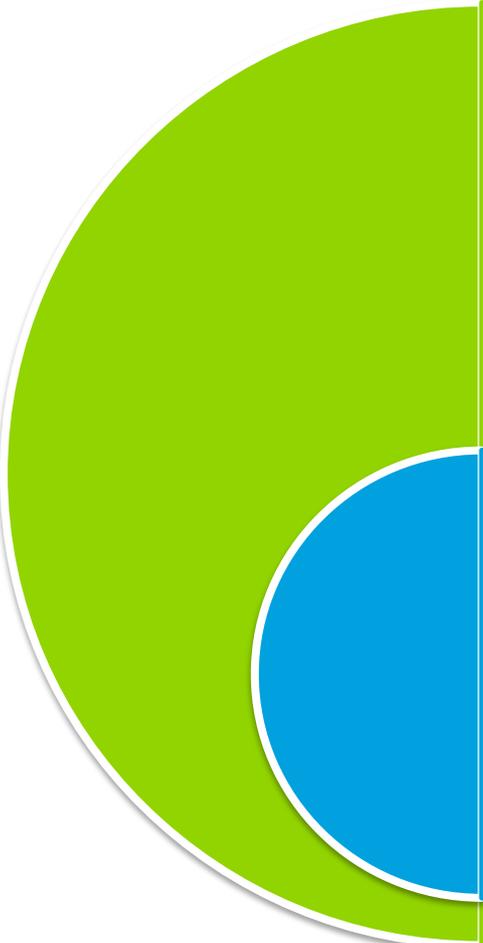
# Why NSTIC?

---

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.**

# Privacy and Civil Liberties are Fundamental

---

## Increase privacy

- Minimize sharing of unnecessary information
- Minimum standards for organizations - such as adherence to Fair Information Practice Principles (FIPPs)
- Focus on privacy-enhancing technologies (PETs)



## Voluntary and private-sector led

- Individuals can choose not to participate
- Individuals who participate can choose from public or private-sector identity providers
- No central database is created

## Preserves anonymity

- Digital anonymity and pseudonymity supports free speech and freedom of association

# 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
- July 2014: NIST awards IDESG Inc. follow-on grant

## Fund Innovative Pilots to Advance the Ecosystem

- Three rounds of pilot grants in 2012 and 2013; **10 pilots now active**
- 3 new awards due next month.

## Government as an early adopter to stimulate demand

- White House effort to create a **Federal Cloud Credential Exchange (FCCX)**
- Last summer: USPS awards FCCX contract; Now: rethink how USG buys identity services
- Next month: FCCX goes live! FedRAMP certified. Rename as “Connect.gov”

---

# Where do we stand?

# The marketplace has started to respond

GADGET LAB

social media

## Twitter Finally Adds Two-Factor Authentication to Secure Your Account

BY ROBERTO BALDWIN 05.22.13 3:36 PM

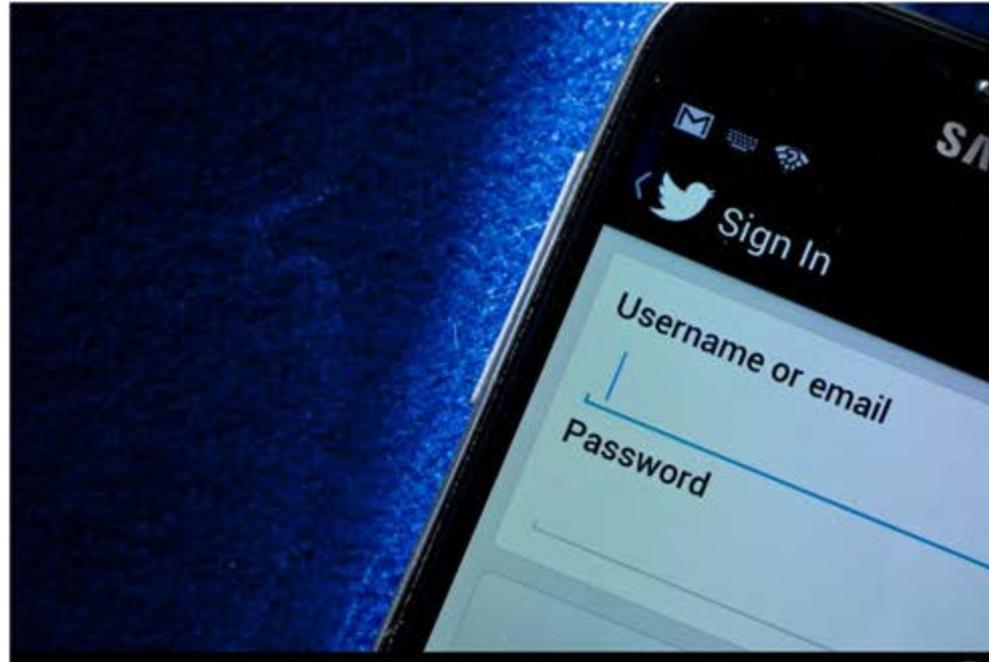
[Follow @strngwys](#)

Share 112

Tweet 539

+1 45

Share 46



# But I now am managing one-off 2FA solutions for

---



# The Good News

---

- **This can be fixed – with a Framework of standards and operating rules that enables interoperability**
- **Both at a technical and policy level**

# The Identity Ecosystem Steering Group



Source: Phil Wolff, <http://www.flickr.com/photos/philwolff/7789263898/in/photostream>

# The Identity Ecosystem Steering Group

---

- 200+ firms/organizations; 60+ individuals
- Elected Plenary Chair (Kim Little 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
  - Policy
  - Privacy
  - Usability
  - Security
  - Trust Frameworks & Trustmarks
  - Health Care
  - Financial Sector
  - International Coordination

# 11 NSTIC Pilots are Advancing the Ecosystem

---

## Three rounds of pilots awarded thus far

- 5 “core” NSTIC pilots in September, 2012; another 4 in September, 2013
- 2 state pilots – focused on improvement of state government services – funded by Partnership Fund for Program Integrity Innovation

***Solicitations took a challenge-based approach focused on addressing barriers the marketplace has not yet overcome***

# NSTIC Pilots Impact

---

More than **140 universities** are deploying **smartphone-based MFA**, thanks to the Internet2 pilot

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

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

A Broadridge/Pitney Bowes JV has launched targeting **140 million customers** for **secure digital delivery** of financial services content, bill presentment and bill pay, enabled by the **ID/Dataweb** identity solution

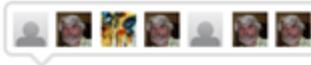
More than **300,000 Veterans** can access online services from more than **70 organizations** without having to share documents containing sensitive PII to prove Veteran status (**ID.me**)

# Government adoption advancing

Forbes

TECH | 8/21/2013 @ 7:49AM | 18,278 views

## Ditch Your Passwords -- USPS Service Enables Online Access to Multiple Federal Agencies



21 comments, 13 called-out

[+ Comment Now](#)

[+ Follow Comments](#)

[SecureKey](#), based in Toronto, today announced it has been awarded a contract by the USPS to provide a cloud-based authentication infrastructure.

Get ready for a new set of abbreviations. This is part of some federal programs that have been underway for several years, mostly below the radar — at least this is the first I have heard of it despite being an avid reader of tech publications. But apparently a lot of people have been working on this — some of the relevant Web sites and information sources are listed below.

The Federal Cloud Credential Exchange (FCCX) is designed to enable individuals to securely access online services —such as health benefits, student loan information, and retirement benefit information—at multiple federal agencies without the need to use a different password or other digital identification for each service. The first federal agency to use it will be the [Veterans Administration](#)

---

# Trust matters to online business

**\$2  
Trillion**

The total  
projected  
online retail  
sales across  
the G20  
nations in  
2016

**\$2.5  
trillion**

What this  
number can  
grow to if  
consumers  
believe the  
Internet is  
more worthy  
of their trust

**\$1.5  
Trillion**

What this  
number will  
fall to if Trust  
is eroded

Source: *Rethinking Personal Data: Strengthening Trust*. World Economic Forum, May 2012.