National Strategy for Trusted Identities in Cyberspace

Michael Garcia

NIST

May 10, 2011

Safeguarding Health Info through HIPAA

What is NSTIC?

Individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

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."

Guiding Principles

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

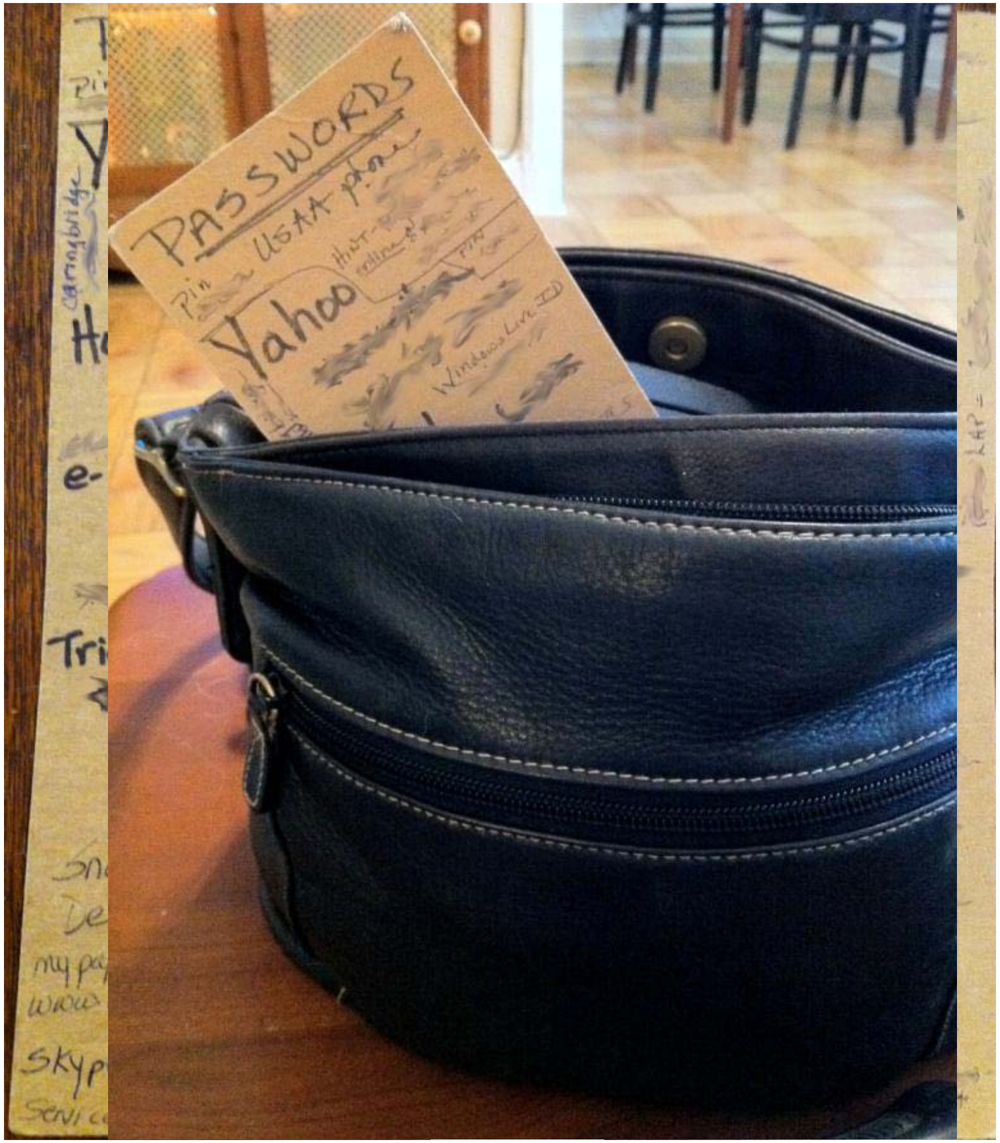
Called for in President's Cyberspace Policy Review (May 2009):
a "cybersecurity focused identity management vision and strategy"

The Problem Today

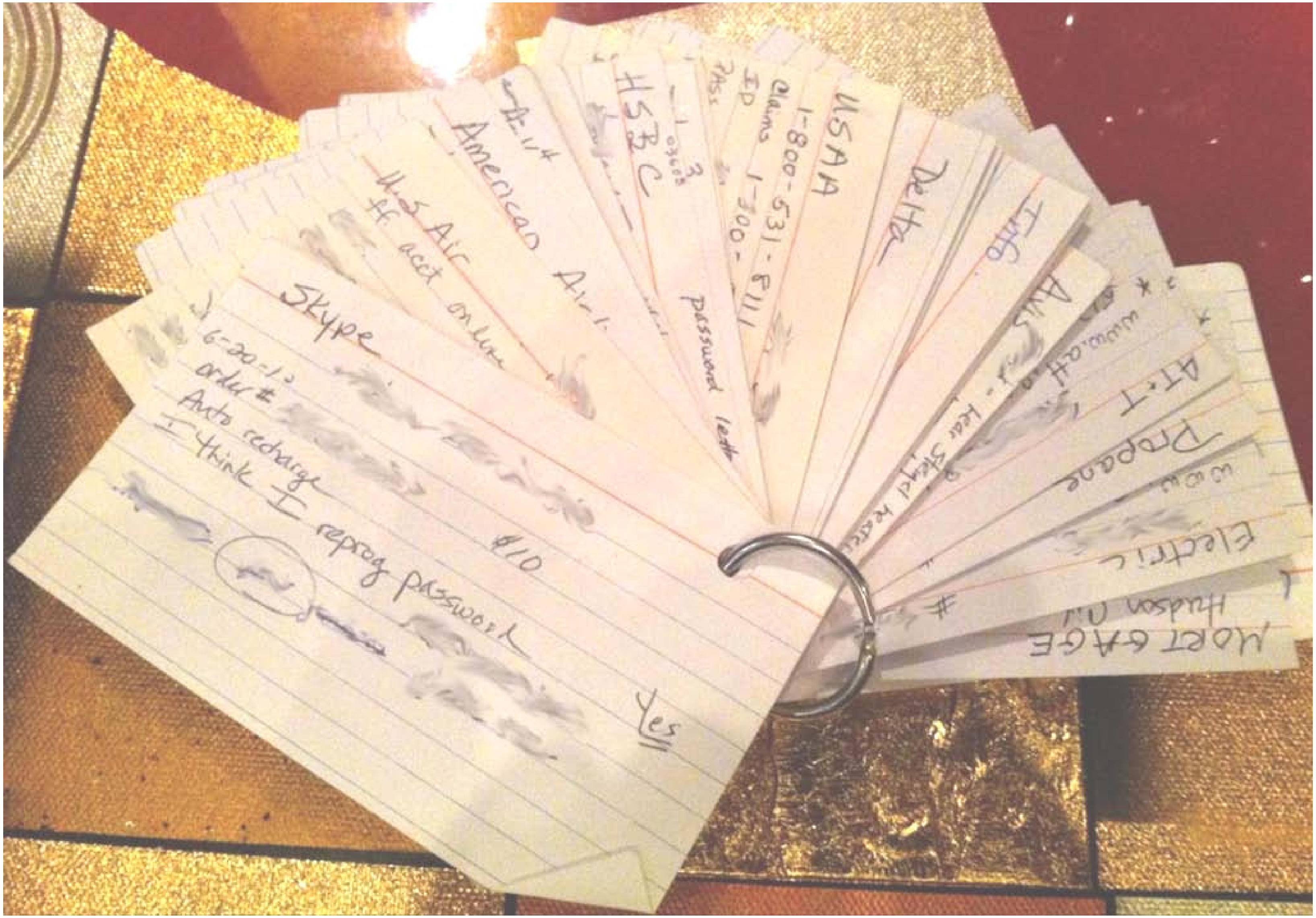
Usernames and passwords are broken

- Most people have 25 different passwords, and often reuse them
- Strong passwords are vulnerable…criminals can get the "keys to the kingdom"
- Rising costs of identity theft
  - 123% increase in financial institution Suspicious Activity Reports in last 6 years (FINCEN)
  - 11.7 million est. victims over 2 years (BJS, 2008)
  - $17.3 billion est. cost to economy over 2 years (BJS, 2008)
- Cybercrime is also on the rise
  - Incidents up 22% from 2009 to 2008 (IC3 report)
  - Total loss from these incidents up 111%, to $560 million

No Seriously, There's a Problem Today



There's a Problem Today, Travel Edition

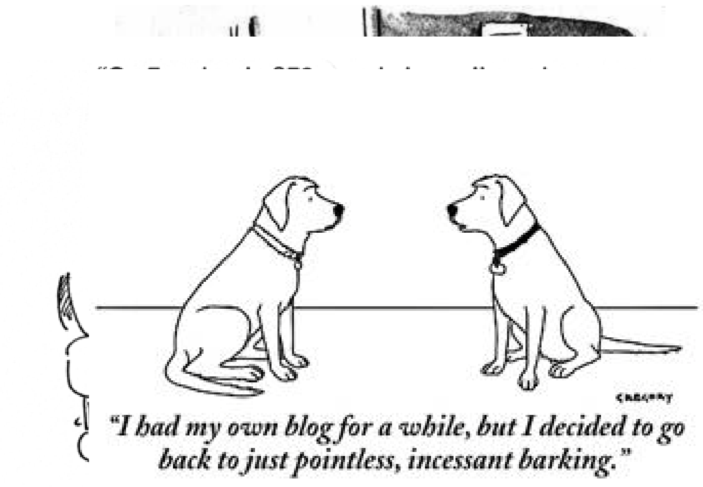


The Problem Today

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



"I had my own blog for a while, but I decided to go back to just pointless, incessant barking."

New Yorker, July 5, 1993 Rob Cottingham, September 23, 2005

- Many transactions, such as signing an auto loan or a mortgage, are still considered too risky to conduct online due to liability risks

The Problem Today

Privacy remains a 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

- Individuals have few practical means to control use of their information

NEW YORK STATE

ENHANCED DRIVER LICENSE

ID: 012 345 678 CLASS D

DOCUMENT
SAMPLE, LICENSE
2345 ANYPLACE AVE
ANYTOWN NY 12345

DOB: 06-09-85

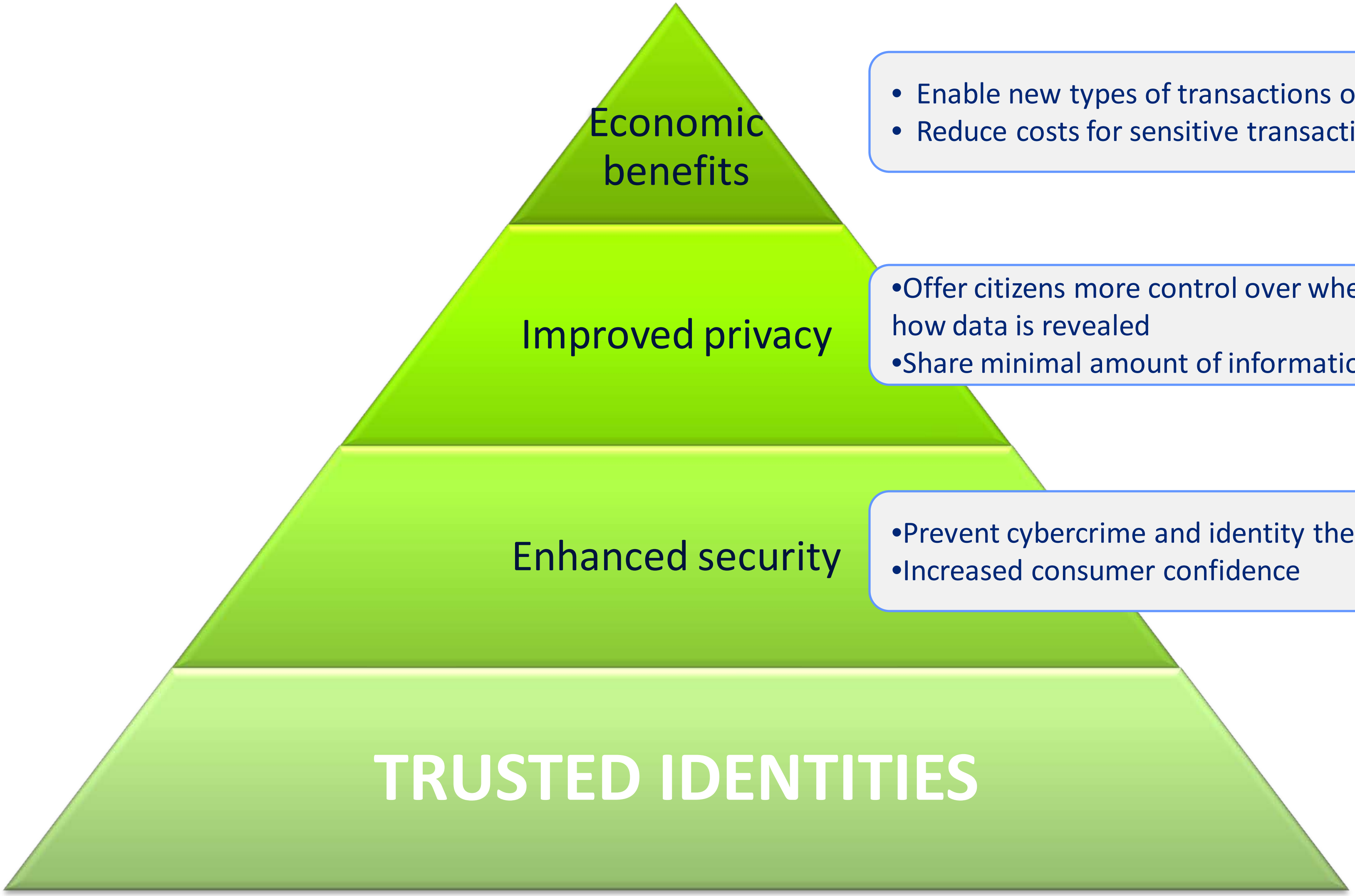
SEX: F EYES: BR HT: 5-09

E: NONE

R: NONE

ISSUED: 09-30-08 EXPIRES: 10-01-16

Trusted Identities provide a foundation



- Enable new types of transactions online
- Reduce costs for sensitive transactions

•Offer citizens more control over when and how data is revealed

•Share minimal amount of information

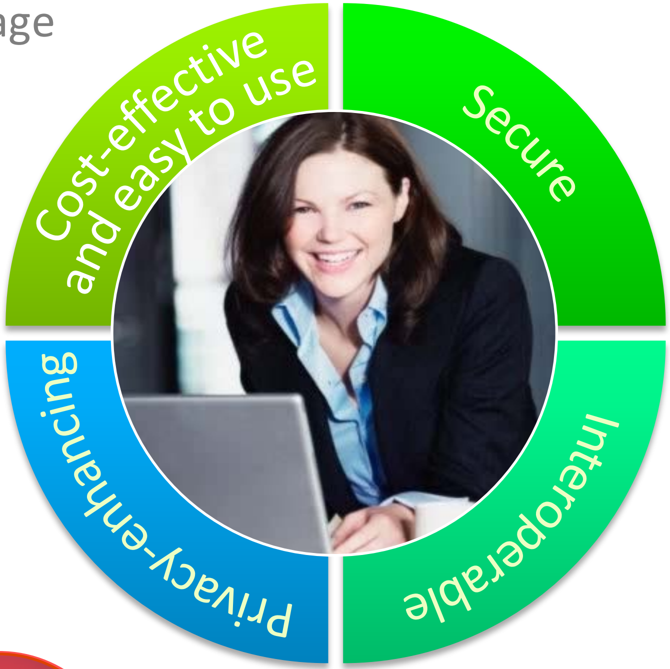
•Prevent cybercrime and identity theft

•Increased consumer confidence

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.

Sign mortgage with digital signature



Cost-effective and easy to use

Secure

Interoperable

Privacy-enhancing

Alternative payment mechanisms; convenient transactions

Trustworthy critical service delivery

Single Sign-On to her corporate portal

Security ‘built-into’ the system to reduce user error

Surf and communicate anonymously or pseudonymously

We've proven that Trusted Identities matter

Major Security Impact

- DoD network intrusions fell 46% after it banned passwords for log-on and instead mandated use of the CAC with PKI.

But Barriers Exist

- High assurance credentials come with higher costs and burdens
- They’ve been impractical for many organizations, and most single-use applications.
- Metcalfe’s Law applies – but there are barriers (standards, liability, usability) today that the market has struggled to overcome.

What does NSTIC call for?

Private sector will lead the effort

- Not a government-run identity program
- Industry is in the best position to drive technologies and solutions
- Can identify what barriers need to be overcome

Federal government will provide support

- Help develop a private-sector led governance model
- Facilitate and lead development of interoperable standards
- Provide clarity on legal framework around liability and privacy
- Act as an early adopter to stimulate demand

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)

Voluntary and private-sector led

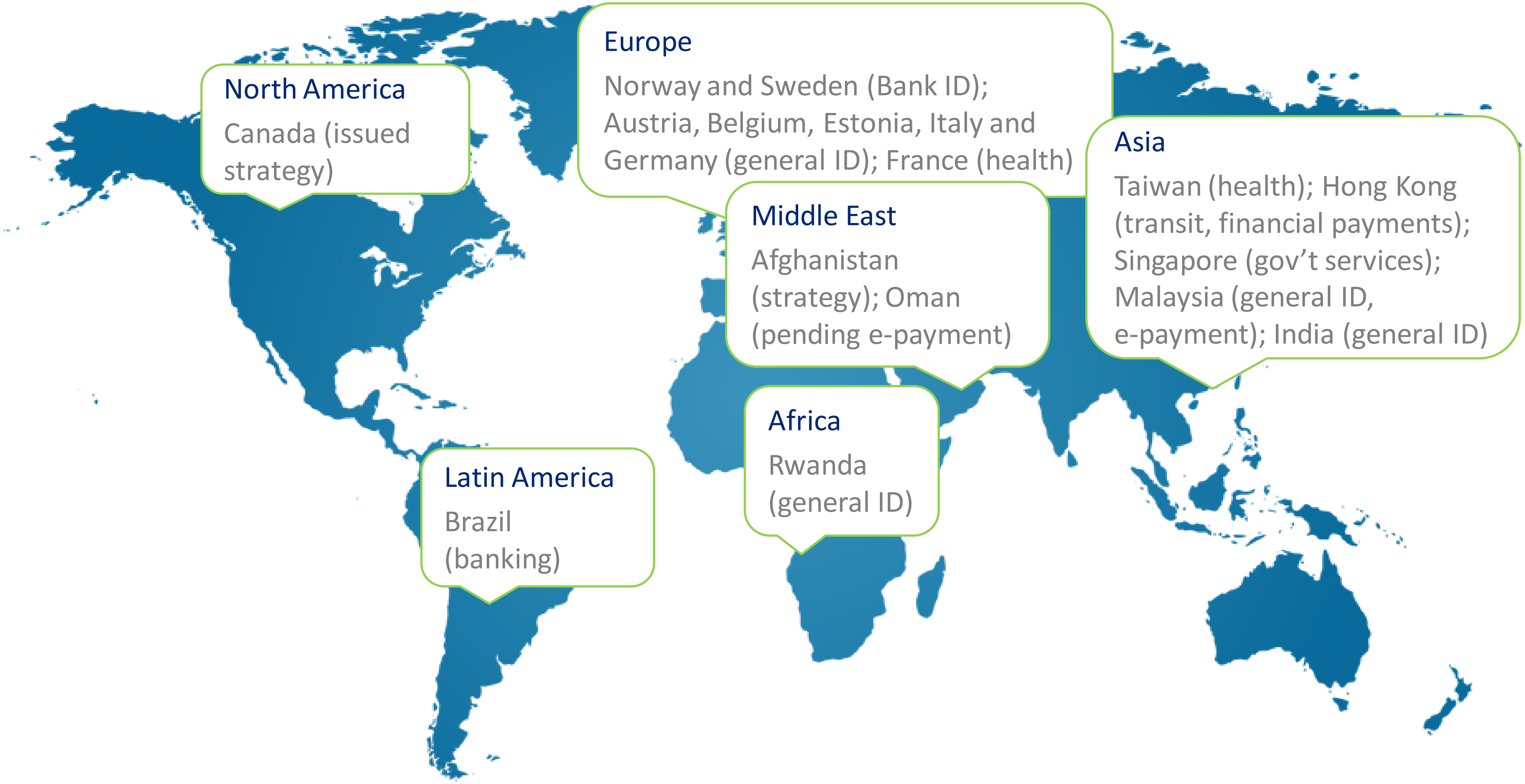
- Individuals can choose not to participate
- Individuals who participate can choose from public or private-sector identity providers
- No central database is created

Preserves anonymity

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

Other countries are moving forward

NSTIC is unique in that it is led by the private sector.



North America

Canada (issued strategy)

Europe

Norway and Sweden (Bank ID); Austria, Belgium, Estonia, Italy and Germany (general ID); France (health)

Asia

Taiwan (health); Hong Kong (transit, financial payments); Singapore (gov't services); Malaysia (general ID, e-payment); India (general ID)

Middle East

Afghanistan (strategy); Oman (pending e-payment)

Africa

Rwanda (general ID)

Latin America

Brazil (banking)

Industry and Privacy Support

The eCitizen Foundation applauds the Administration's development of NSTIC as a major advance in meeting the needs for citizen control of personal information, privacy protections and security. With the strong citizen-centered approach envisioned by NSTIC, a vibrant marketplace fostering innovative solutions will be possible.

Dan Combs, CEO, eCitizen

The improved online identities resulting from NSTIC can help address concerns about identity theft, online fraud, intellectual property, privacy and cybersecurity without creating a centralized or government-managed system.

Phil Bond, President and CEO, TechAmerica

The NSTIC addresses one of the thorniest issues facing those who want to engage in significant or sensitive online transactions: the lack of standard, interoperable, and trusted policies and procedures for proving online identity. The process initiated by the NSTIC serves a critical need by helping to tackle these legal challenges in the first integrated public-private effort of its kind.

Thomas Smedinghoff, Co-Chair,
American Bar Association ID Management Legal Task Force

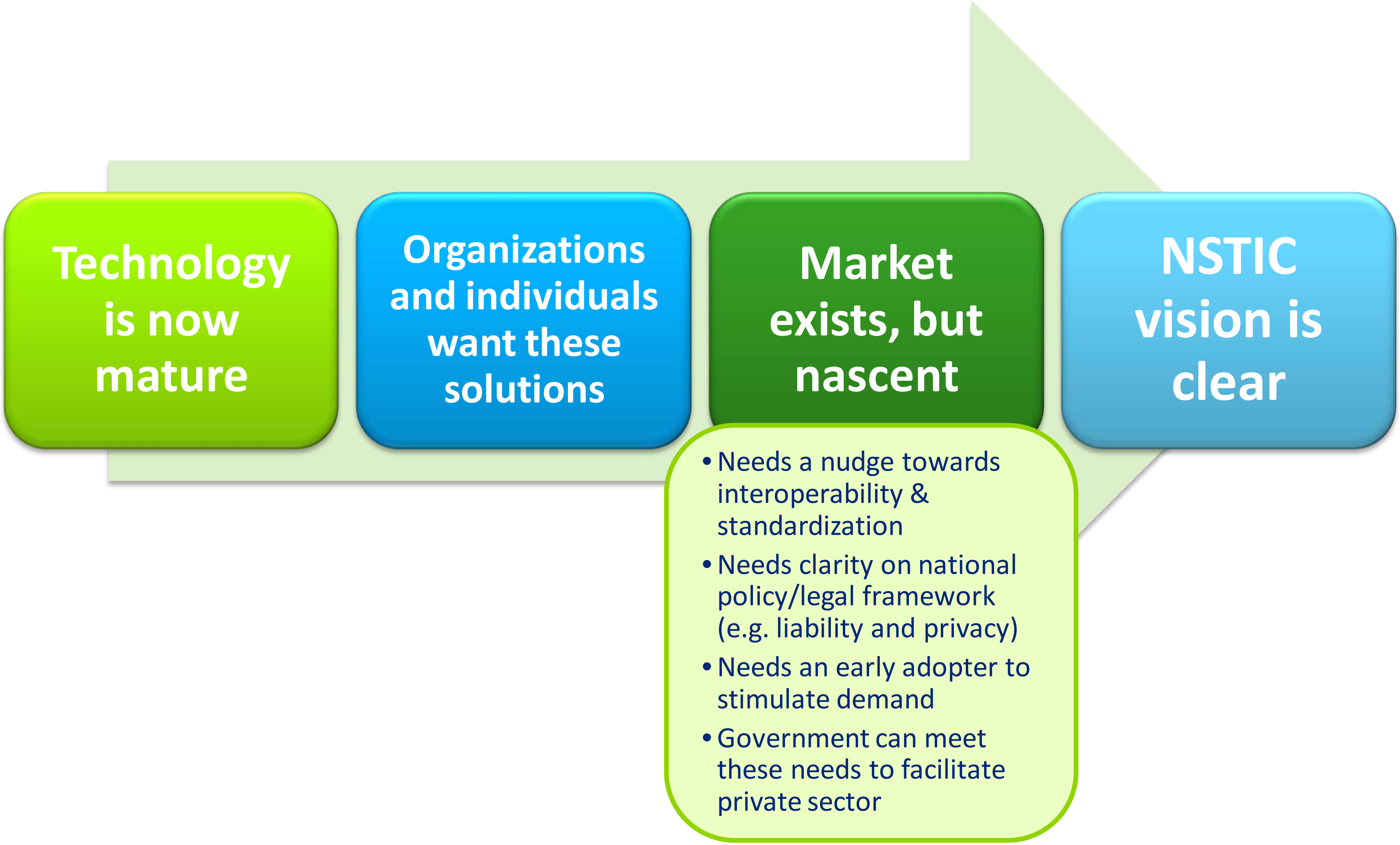
NSTIC has the opportunity to tip the balance of the conversation and focus on identity to socio-economic benefit from what is often today one of identity fraud and identity theft. In doing so trusted identities can improve the delivery and lower the cost to the public of financial services, health care, e-commerce and reduce the federal budget.

Salvatore D'Agostino, CEO, Idmachines LLC

I have been praising the Administration for promoting improvements in online identity that would address concerns about identity theft, online fraud and cybersecurity without creating a centralized or government-managed system.

Jim Dempsey, VP for Public Policy, Center for Democracy & Technology

The Time is Now



Technology is now mature

Organizations and individuals want these solutions

Market exists, but nascent

NSTIC vision is clear

- Needs a nudge towards interoperability & standardization
- Needs clarity on national policy/legal framework (e.g. liability and privacy)
- Needs an early adopter to stimulate demand
- Government can meet these needs to facilitate private sector

Next Steps: Workshops

Workshops in 2011

- Workshop 1: Governance
  - Early June; 2 days in Washington, DC; open to public
  - Focus on structures, baseline functionality, basic membership and certification requirements
- Workshop 2: Privacy and Usability
  - Early Summer; 2 days in Boston, MA; open to public
  - Focus on ways to embed FIPPs in Identity Ecosystem; requirements building for different parties; methods of establishing user-centric privacy environment
- Workshop 3: Technology and Standards
  - September; 2 days in Bay Area; open to public
  - Focus on standards and specification identification and harmonization needs; adopting standards that fostering innovation

Next Steps: Priorities

Focus in 2011

- Establish Governance model
  - Private sector led; multi-stakeholder collaboration
  - Enable expedited focus on consensus standards and operating rules
  - Explore models for addressing liability
- Pilots:
  - Develop criteria for selection
  - Assess potential programs
  - Prepare for formal pilot launches with funding in FY12

Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap
- Increased adoption of Trust Framework Providers (TFPs)

The Role for the Health and Civil Rights Communities

Participate

- Workshops
- Governance
- Pilots

Continued Focus

- Risk-management for authentication and privacy and security as complimentary
- Continue to improve and enhance partnerships, drive innovation

Give us your ideas!

- You are a key partner, we want to hear from you!

Questions?

For info and news, and to sign up receive updates

www.nist.gov/nstic

nstic@nist.gov

Jeremy Grant

jgrant@nist.gov

202.482.3050

Mike Garcia

michael.garcia@nist.gov

202.590.0979