

# National Strategy for Trusted Identities in Cyberspace

Jeremy Grant  
NIST



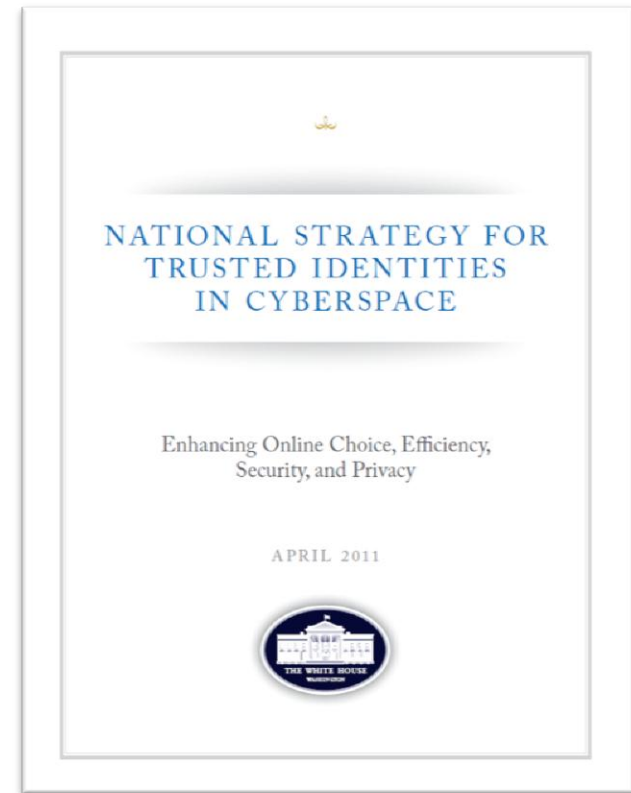
# What is NSTIC?

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.”



# The Problem Today

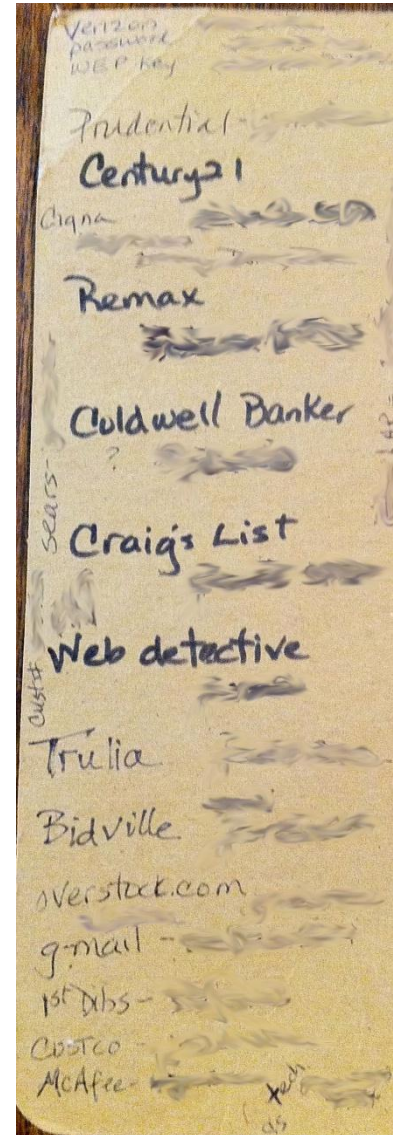
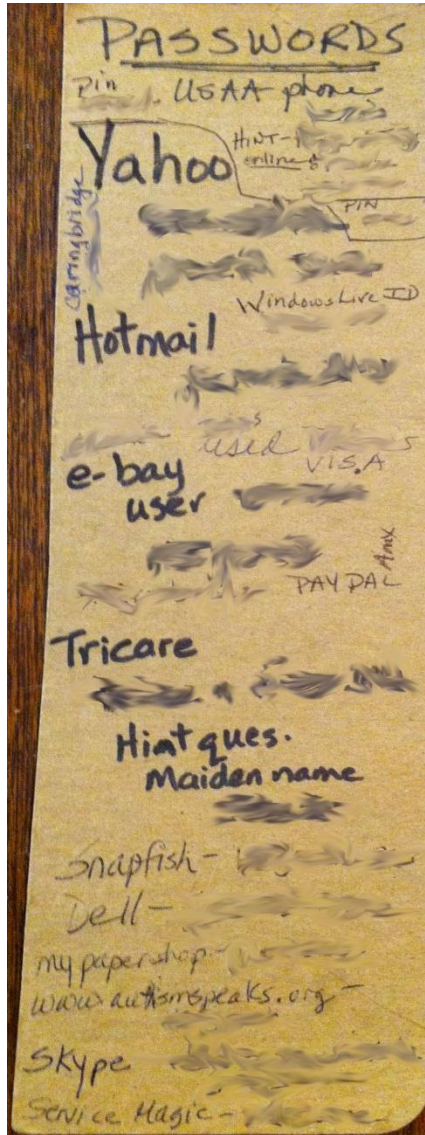
---

## Usernames and passwords are broken

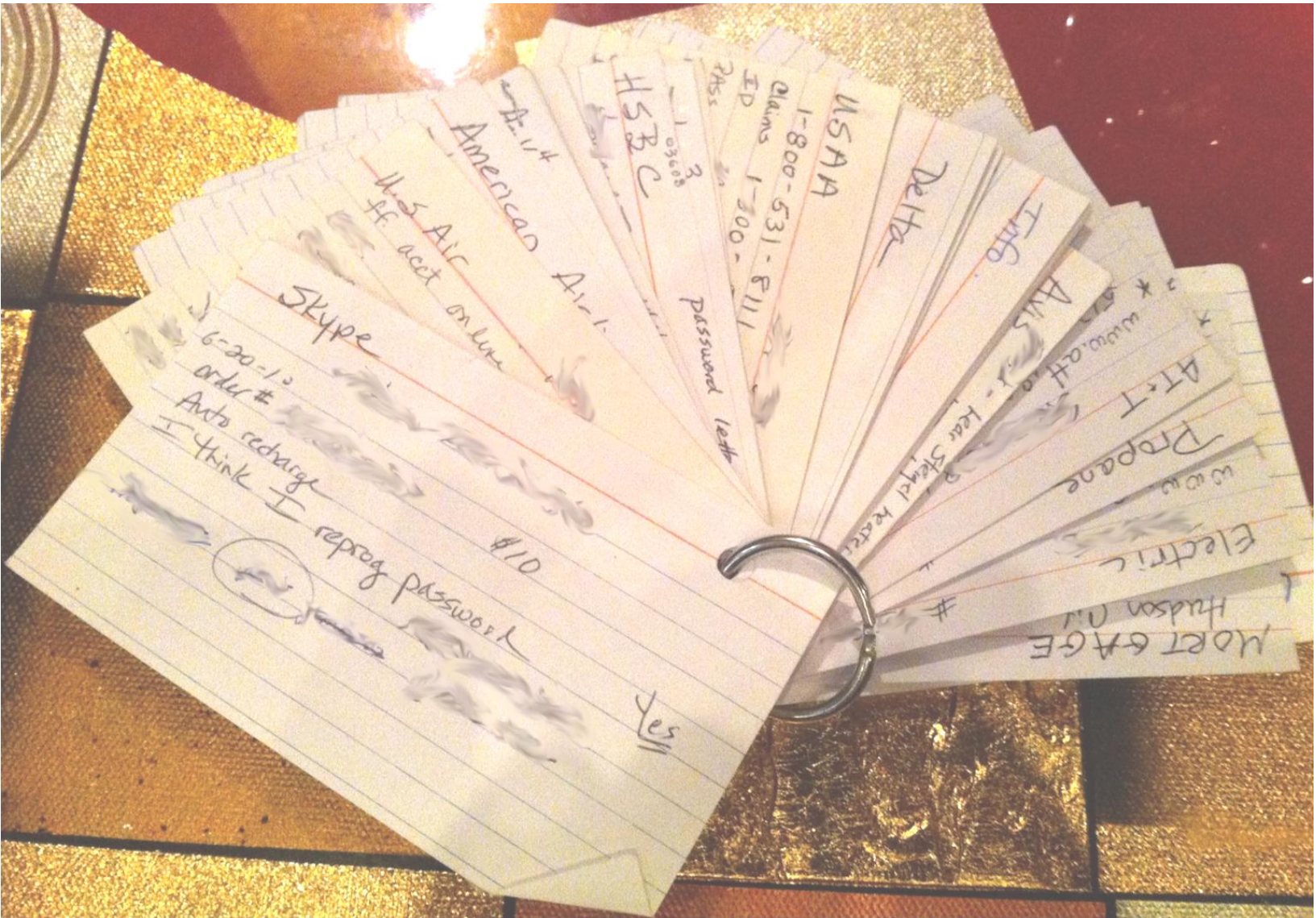
- Most people have 25 different passwords, or use the same one over and over
- Even strong passwords are vulnerable...criminals can get the “keys to the kingdom”
- Rising costs of identity theft
  - 123% increase in financial institution Suspicious Activity Reports in last 6 years (FINCEN)
  - 11.7 million 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



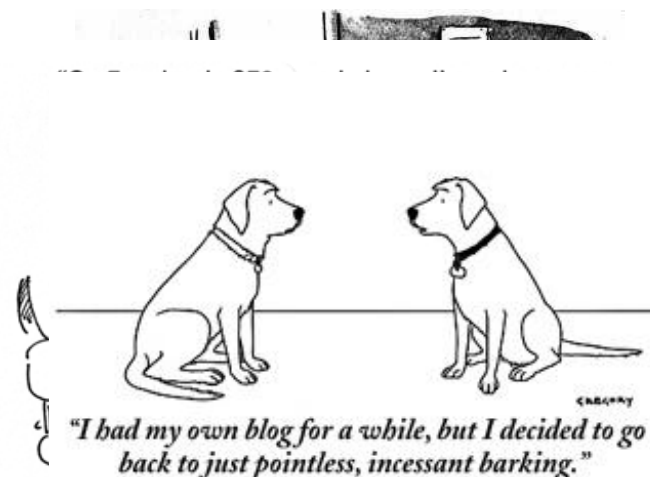
# There's a Problem Today, Travel Edition



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



New York Times, July 5, 2005

# The Problem Today

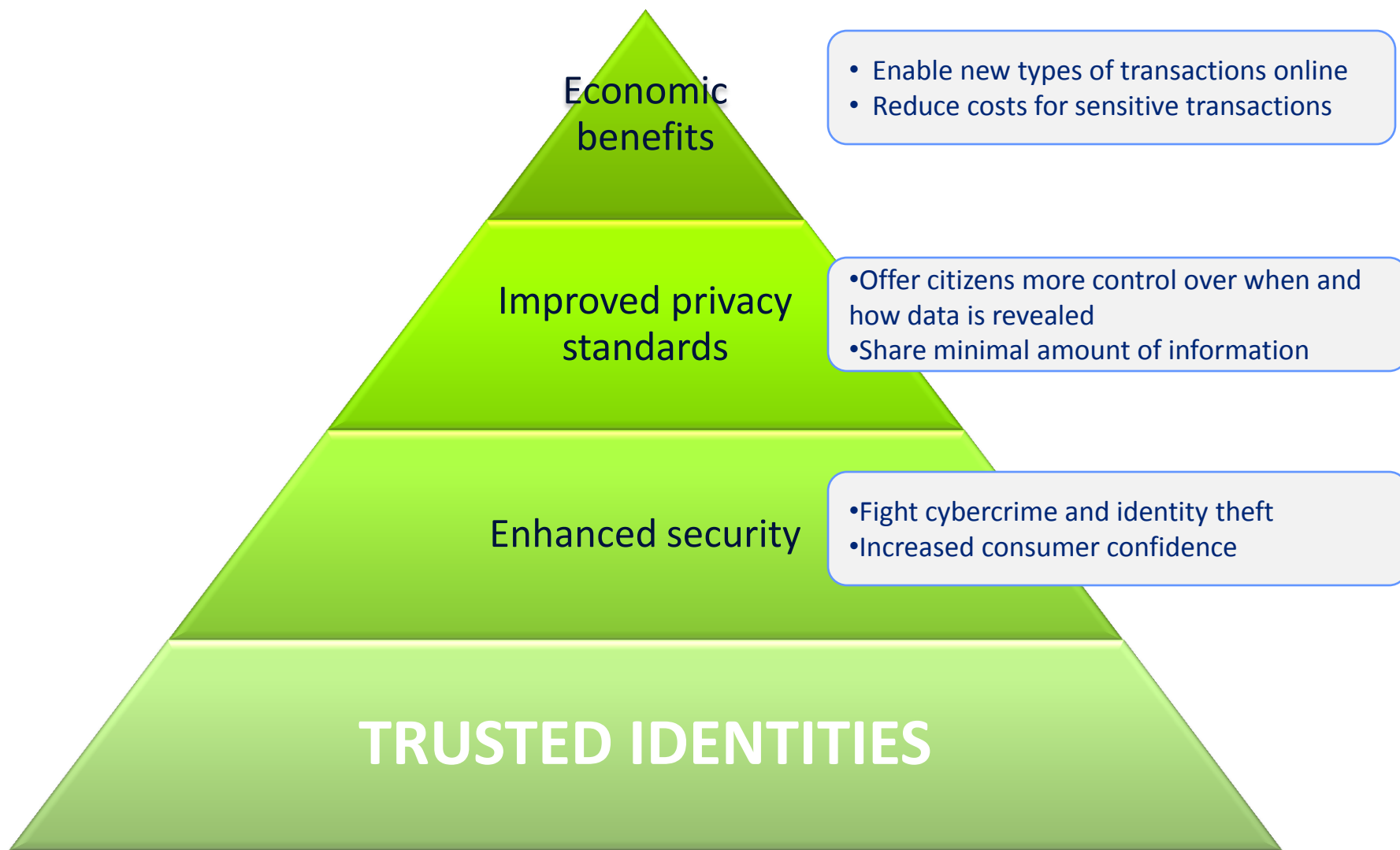
## Privacy remains a challenge

- 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



# 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

# We've proven that Trusted Identities matter

---

## DoD Led the Way

- 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 national policy and 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

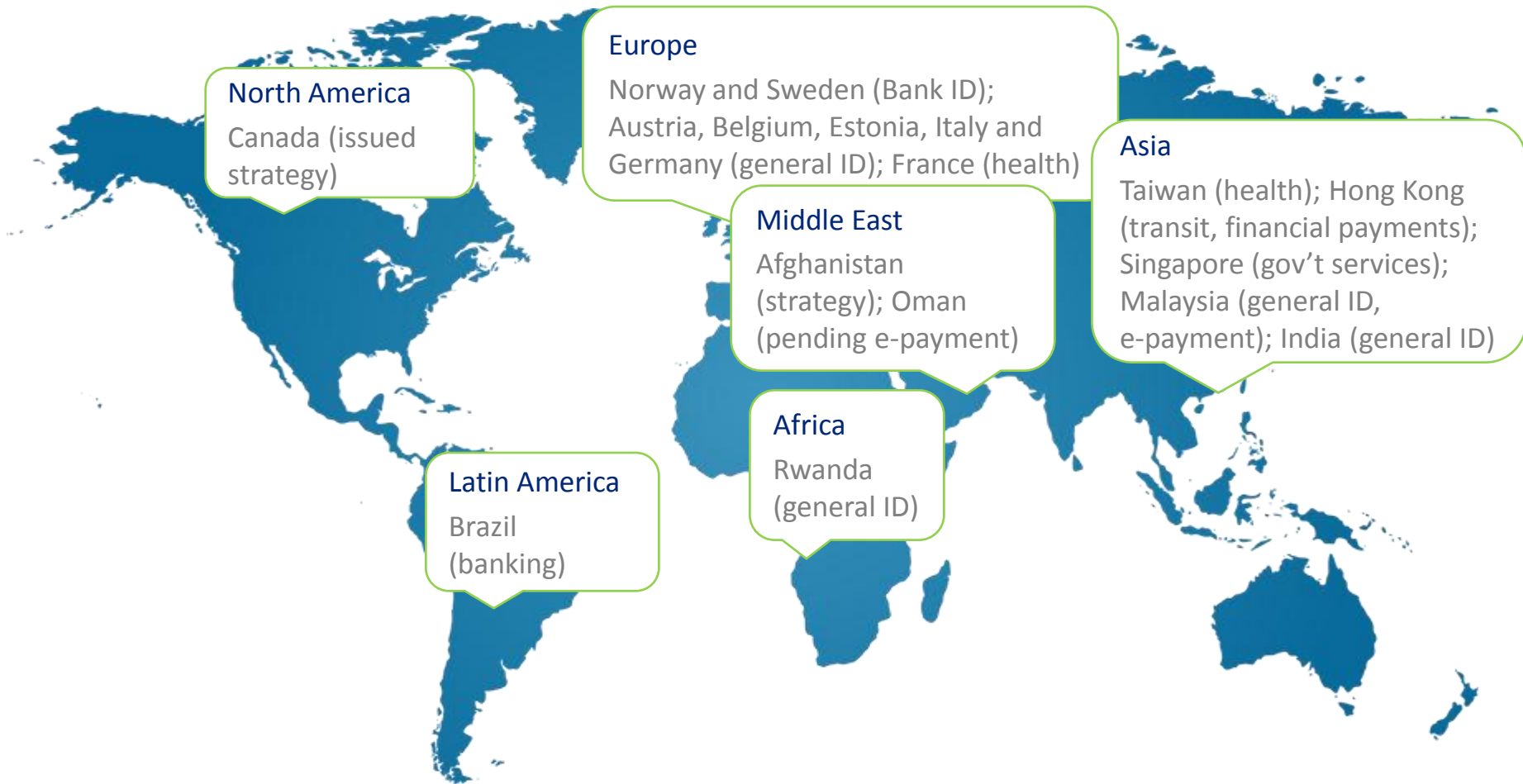
- Individuals can choose not to participate
- Individuals who participate can choose from public or private-sector identity providers
- No central database is created

## 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.



# Industry and Privacy Support

Key members of the U.S. technology industry, the privacy community, and the security industry have expressed support for NSTIC

“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

“The Administration to my view has, has conducted a very open process here....I think that there's a model here perhaps for the broader question of cybersecurity.”

Jim Dempsey, Vice President for Public Policy at the Center for Democracy & Technology

“Our industry strongly supports the goals outlined in the Strategy, and we see a vital role for a National Program office to work with industry and government in its finalization and implementation.”

Letter to Sec. Locke, White House Cybersecurity Coordinator Howard Locke, and Patrick Gallagher from TechAmerica, Business Software Alliance, and Information Technology Industry Council; additional signatures included leadership from Microsoft, Symantec, PayPal, CA, CSC, RSA/EMC, Infineon, Unisys, Verisign and Gemalto and other technology firms



# The Time is Now



# Next Steps

---

## Convene the Private Sector

- Workshops on governance, privacy and technology

## FY11 Focus

- 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 (TFP)

# How you can help

## Participate

- Workshops
- Governance
- Pilots

## Be early adopters

- Leverage trusted identities to move more services online
- Consider ways to support identity proofing and partnerships with private sector

## Give us your ideas!

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

# Questions?

---

Jeremy Grant

[jgrant@nist.gov](mailto:jgrant@nist.gov)

202.482.3050