National Strategy for Trusted Identities in Cyberspace

The Department of Commerce and NSTIC National Program Office

Ari Schwartz

Senior Advisor for Internet Policy

NIST

January 1, 2011

Today's Environment: Complex and Insecure

- High-value services that could be online are still manual and in-person
- Inefficiency costs are passed onto individuals

- Individuals' physical locations are vulnerable
- Criminals harvest valuable information like mother's maiden names or pets' names to defeat authentication questions for other high-value transactions.

- Individuals must make trade-offs with their data security and privacy
- Individuals re-use passwords in order to remember them
- Snoopers on the network have the "keys to the kingdom"

- "Phishing" leads to raided bank accounts and unauthorized charges on credit cards.
- "Phishing" websites look so much like legitimate sites the average individual can't tell the difference.

- Unnecessary helpdesk costs
- Password reset mechanisms default to publicly available data such as 'mother's maiden name'
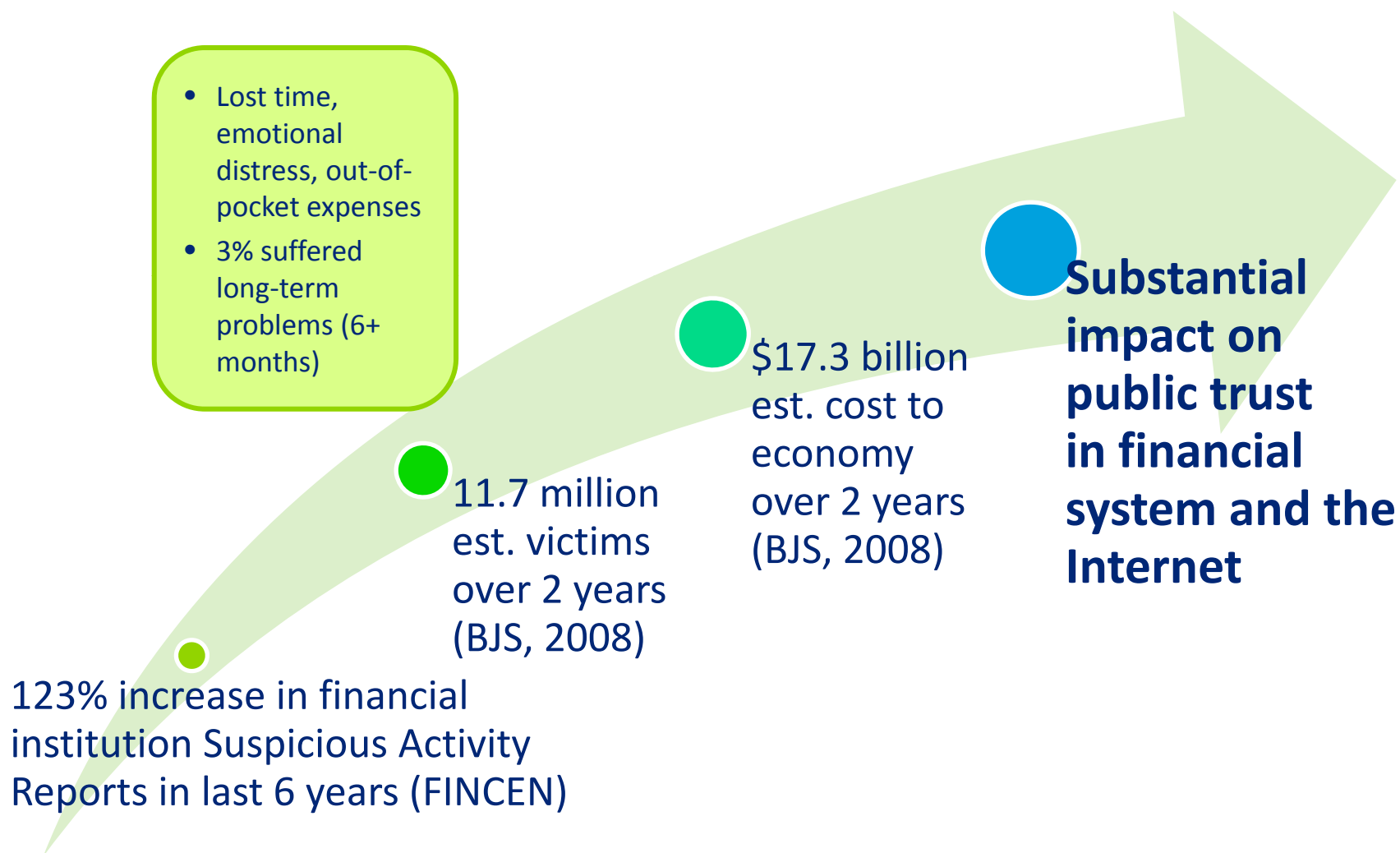
- Industries like Health IT rely on username/passwords, risking massive data breaches
- Long-term setbacks if privacy failures undermine public trust

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

Trustworthy critical service delivery

Security 'built-into' the system to reduce user error

Cost-effective and easy to use

Secure

Privacy-enhancing

Interoperable

Alternative payment mechanisms; convenient transactions

Single Sign-On to her corporate portal

Privately post location to her friends

National Strategy for Trusted Identities in Cyberspace

National Cost: The Toll Of Identity Theft

- Lost time, emotional distress, out-of-pocket expenses
- 3% suffered long-term problems (6+ months)

11.7 million est. victims over 2 years (BJS, 2008)

$17.3 billion est. cost to economy over 2 years (BJS, 2008)

Substantial impact on public trust in financial system and the Internet

123% increase in financial institution Suspicious Activity Reports in last 6 years (FINCEN)

National Strategy for Trusted Identities in Cyberspace

National Savings:
Identity Solutions Increase Efficiency and Productivity

More efficient government

- **$105 million** projected savings over 3 years at USDA
- Est. $480 savings per user at National Cancer Institute (CTET pilot)

More efficient industry

- Cancer research (CTET pilot)
  - Less time on paperwork, **more time in the lab**
  - 3.3 million pages not printed

More productive employees

- Save 15 minutes/day (previously spent logging-in to various systems/apps)
- Time savings average 3,750 extra hours of productivity per day for 15,000 users

National Strategy for Trusted Identities in Cyberspace

Problem: Lack of Mutual Trust on the Internet

Risky

- Businesses use inefficient and duplicative identification processes to protect against fraud and identity theft
- Individuals can't tell if websites are legitimate
- Even National critical infrastructure insecure
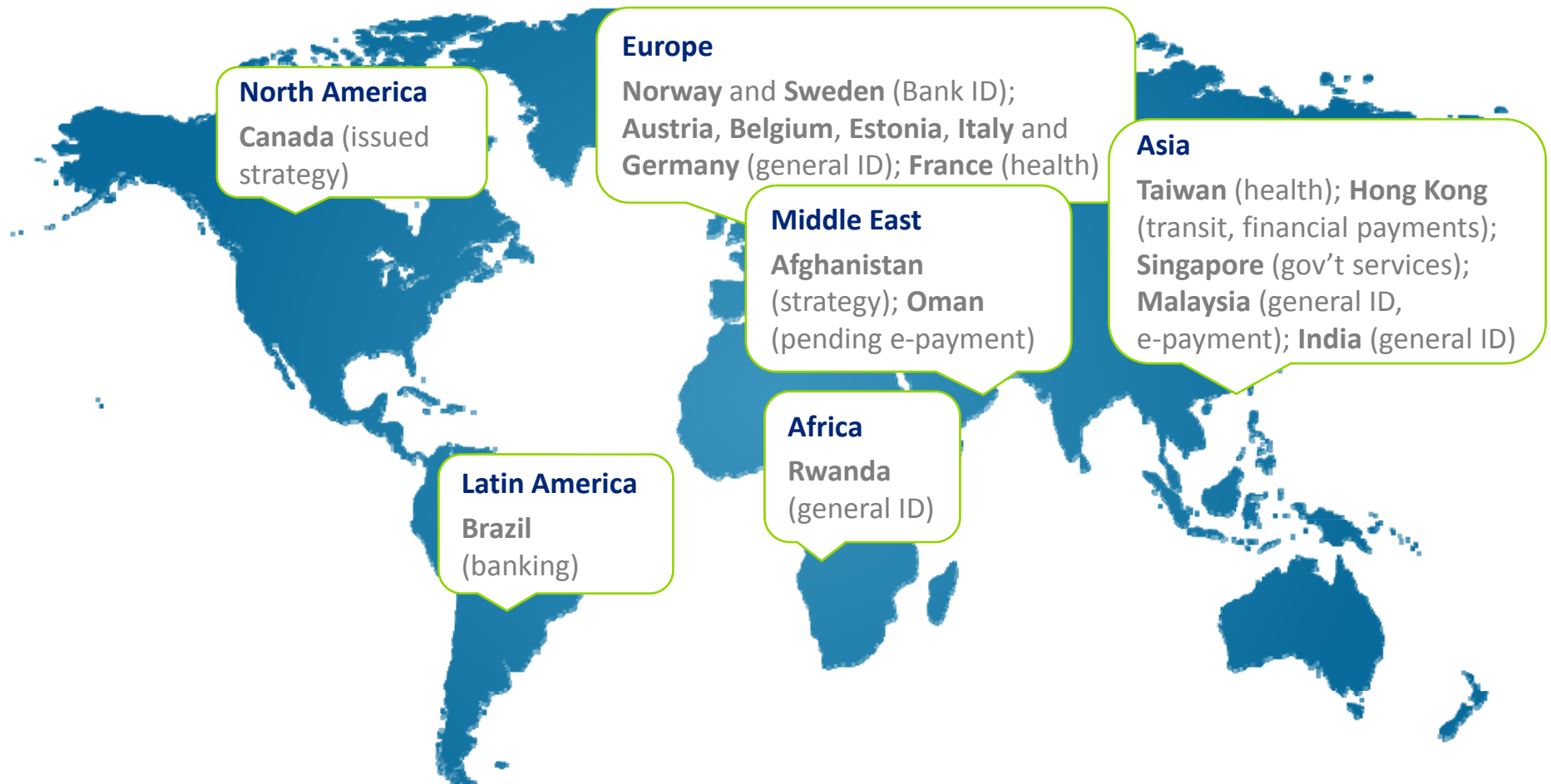 - Cannot secure networks unless we can better identify hardware

Inconvenient

- Multiple user name/passwords → weak passwords get re-used → easily compromised → consumer fear/caution using Internet

Lagging Behind

- E-commerce and government services are limited due to risk
- Other nations are moving ahead with ideas that will not spur innovation

National Strategy for Trusted Identities in Cyberspace

Online ID Efforts Around the World

North America
Canada (issued strategy)

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

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

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

Latin America
Brazil (banking)

Africa
Rwanda (general ID)

National Strategy for Trusted Identities in Cyberspace

Solution: Trusted Identities

Secure

- Fight identity theft
- Increase consumer confidence to do business online
- Identification of hardware and software to secure critical infrastructure

Convenient

- Individuals can easily access online services

Innovation and Growth

- Platform for innovation and new businesses
- Enables industry to move more services online

Privacy and Civil Liberties are Fundamental

Increase privacy

- Minimize sharing of unnecessary information
- Minimum standards for organizations
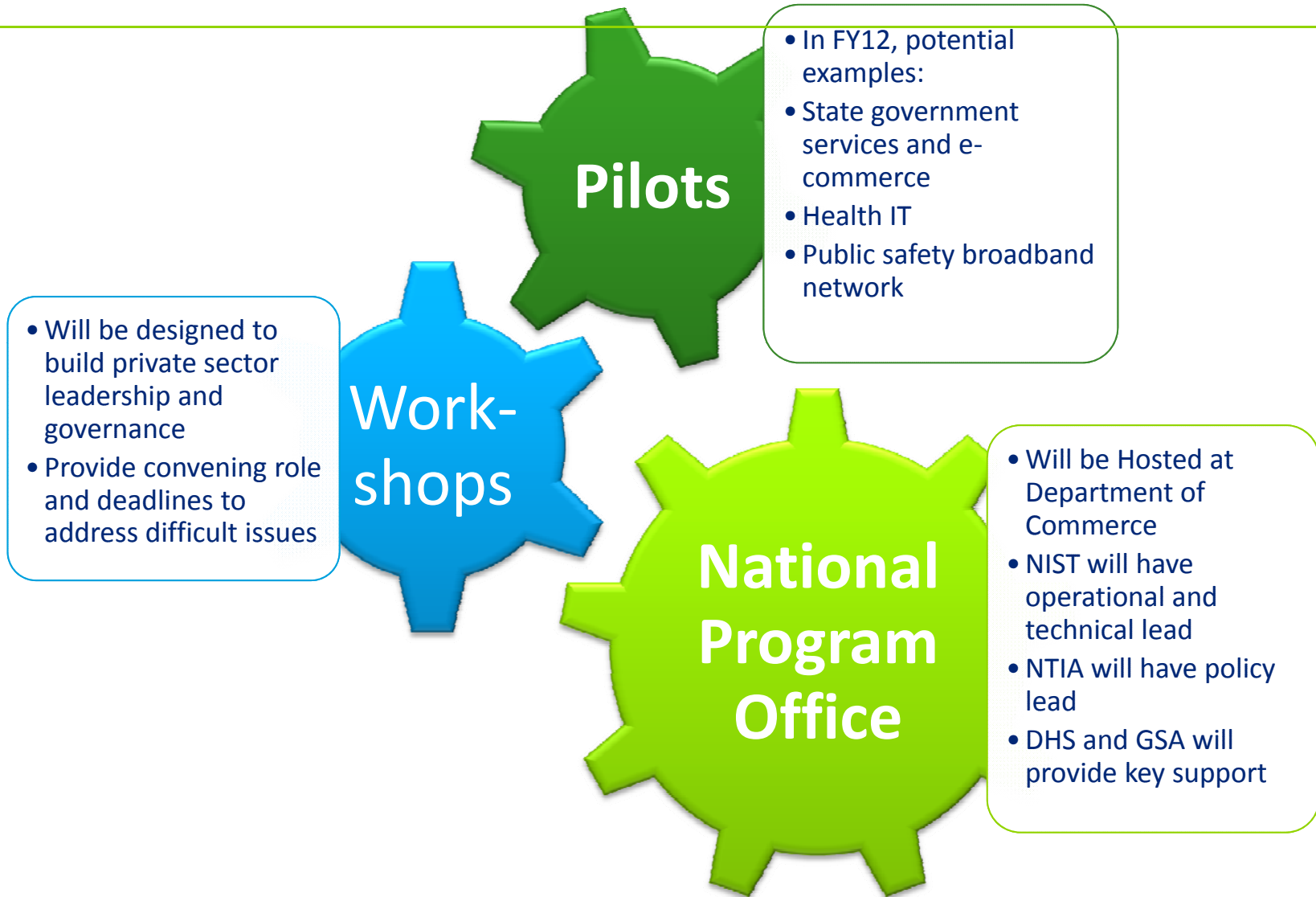
This is NOT a national ID system

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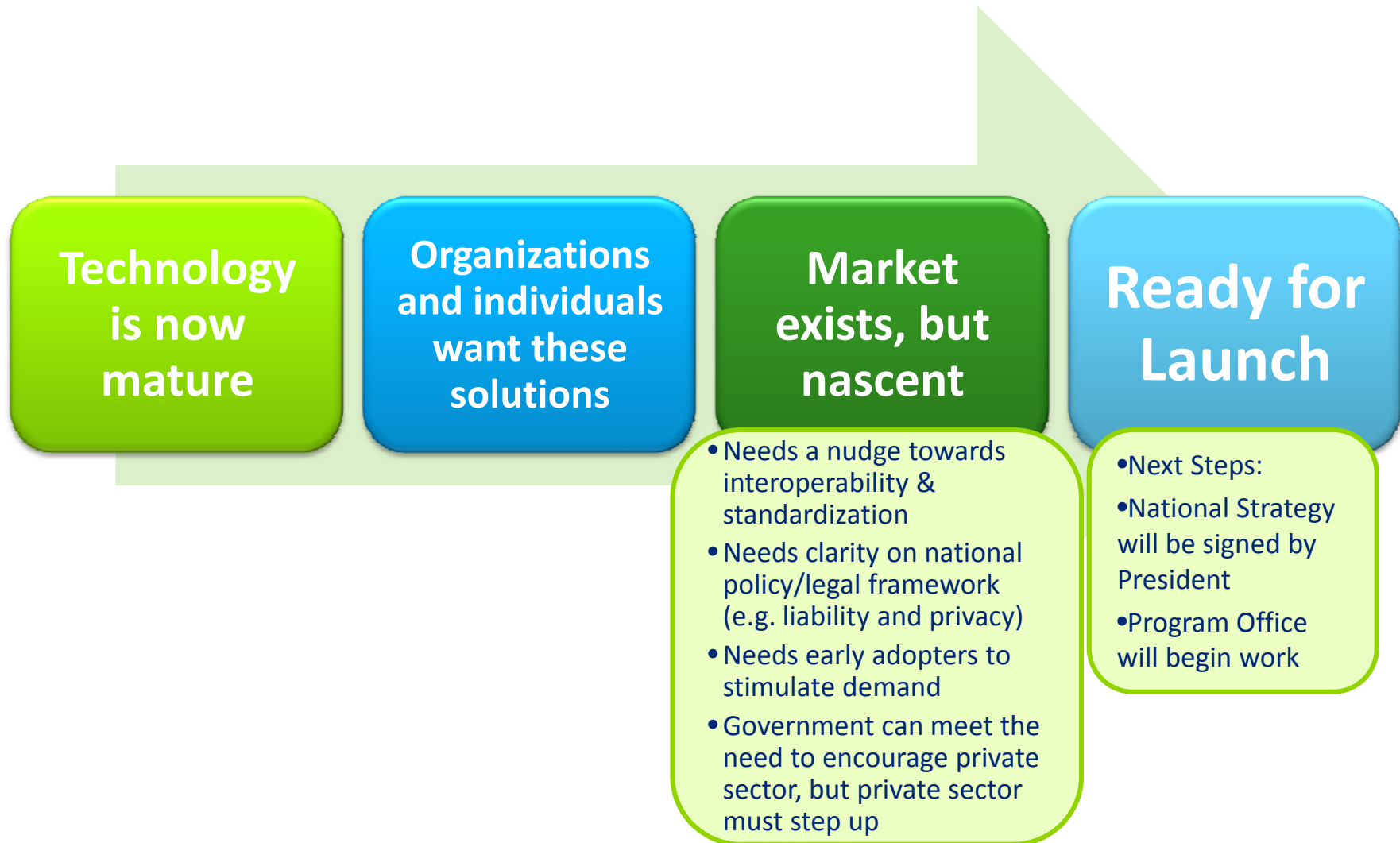- No central database is created

Preserves anonymity

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

National Strategy for Trusted Identities in Cyberspace

Execution Mechanisms

Pilots

- In FY12, potential examples:
- State government services and e-commerce
- Health IT
- Public safety broadband network

Work-shops

- Will be designed to build private sector leadership and governance
- Provide convening role and deadlines to address difficult issues

National Program Office

- Will be Hosted at Department of Commerce
- NIST will have operational and technical lead
- NTIA will have policy lead
- DHS and GSA will provide key support

The Time is Now

Technology is now mature

Organizations and individuals want these solutions

Market exists, but nascent

- Needs a nudge towards interoperability & standardization
- Needs clarity on national policy/legal framework (e.g. liability and privacy)
- Needs early adopters to stimulate demand
- Government can meet the need to encourage private sector, but private sector must step up

Ready for Launch

- Next Steps:
- National Strategy will be signed by President
- Program Office will begin work

National Strategy for Trusted Identities in Cyberspace

Combatting Misconceptions about NSTIC

All Americans Will Not be Issued an Internet ID

- This is a voluntary system
- The Government will not require that everyone obtain a digital credential

NSTIC Will Not Enable Privacy Invasive Tracking of People

- NSTIC promotes the use of privacy-enhancing technologies that inhibit the tracking and aggregation of individual's online activities through their digital credentials
- Pilots will be evaluated for privacy-enhancing components

There Will Not Be a Government Run Identity Infrastructure

- The private sector will lead the implementation and management of the Identity Ecosystem
- The Government's role is to facilitate public and private sector activities and ensure consumer protection

National Strategy for Trusted Identities in Cyberspace