The National Strategy for Trusted Identities in Cyberspace (NSTIC): Privacy Overview

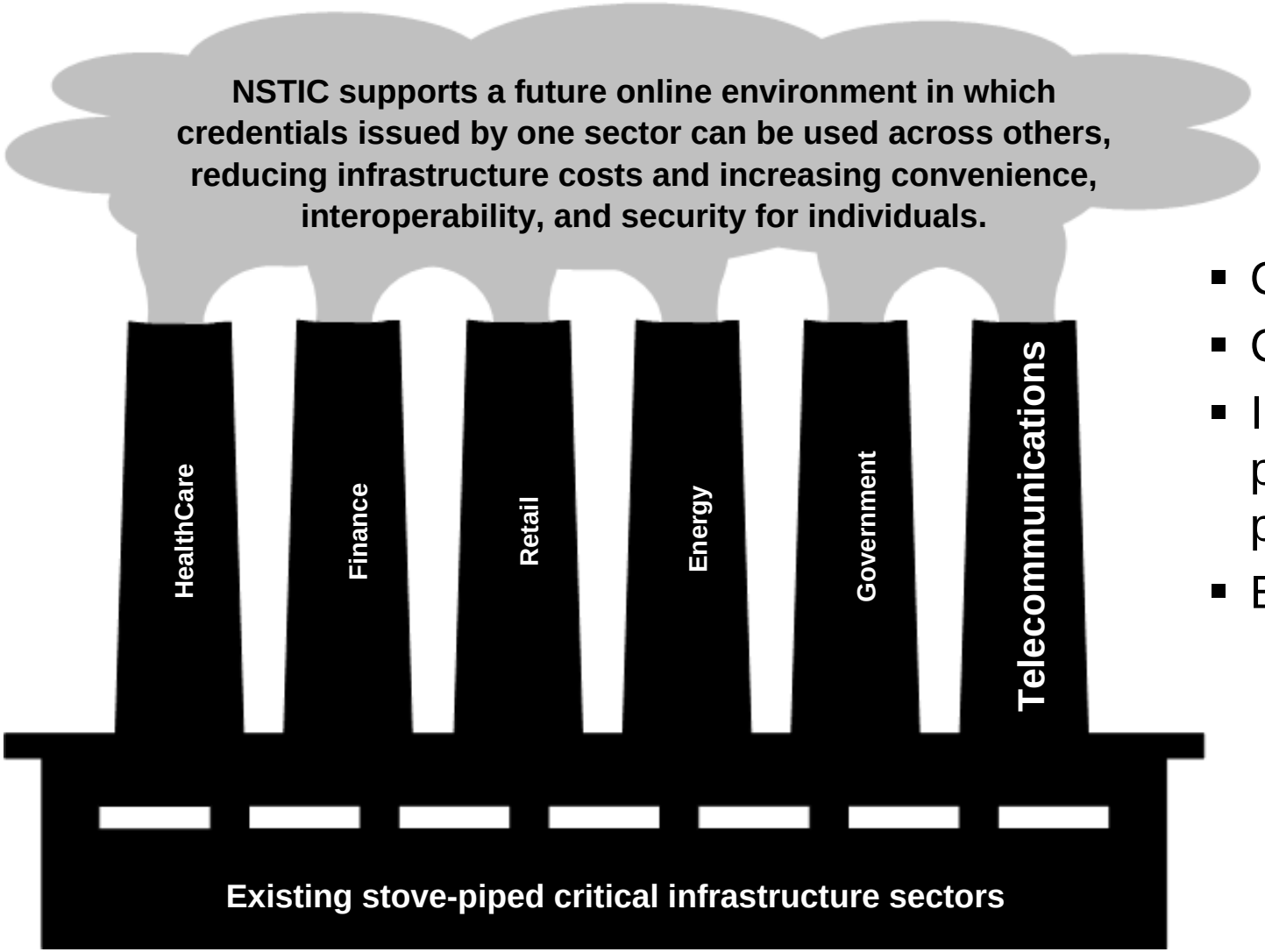
Information Security and Privacy Advisory Board

November 4, 2010

Imagine a World…

An individual learns of a new and more secure way to access online services: his cell phone carrier, bank, and local governments will all offer Identity Ecosystem-approved credentials. He also discovers that his email provider, social networking site, health care provider, and local utility companies accept any of these credentials. He selects the service provider that fits his requirements, and he no longer has to remember dozens of different usernames and passwords.

Coordination of Existing Programs



- Cost savings
- Convenience
- Increased privacy protection
- Efficiency

Benefits

Individual

- **Convenience:** Enabling solutions are intuitive, easily understood, accessible, and widely available.
- **Privacy**: Limiting the amount of identifying information that is collected and transmitted.
- **Security**: Security built-in to well-understood processes and technologies that protect individual interests.

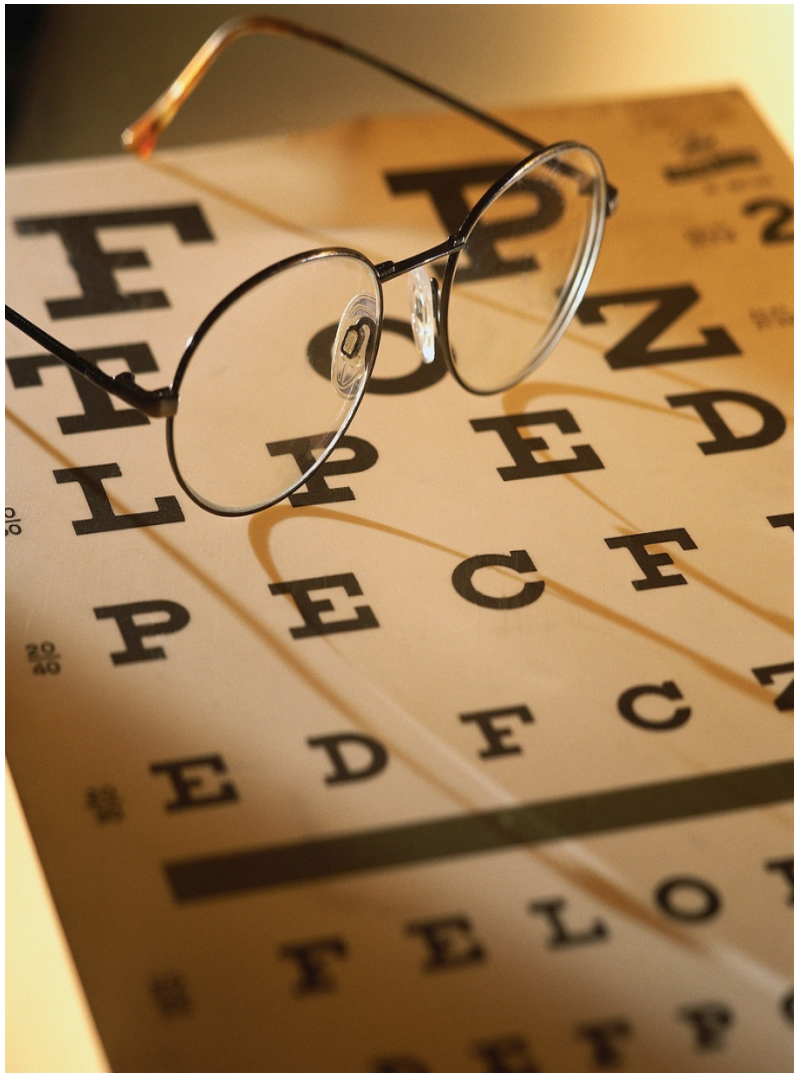
Private Sector

- **Innovation:** Creation of new market opportunities in the form of new and innovative services, particularly those that are higher in risk and user-centric.
- **Efficiency:** Reduction in paper-based processes, help desk costs, and overall increase in productivity; enhanced competitiveness.
- **Trust:** Enhancing the ability to display and protect brands online.

Government

- **Constituent Satisfaction:** Expansion of online services to serve constituents more efficiently and transparently.
- **Economic Stimulation:** Innovation generation through supporting the Identity Ecosystem.
- **Public Safety**: Increased trust leading to a reduction in cyber crime and increased integrity of networks and systems.

The NSTIC Vision



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.

Guiding Principles

- Resilient to change, disruption, or market-driven innovation
- Tolerance to loss, compromise, or theft
- Strong cryptography
- Auditability

- Limitation of data collection
- Minimal linkage
- Data retention
- Protection of anonymity and pseudonymity
- Transparency
- Purpose Specification

- Acceptance of multiple credentials
- Supports identity portability
- Encourages non-proprietary standards
- Modularity, flexibility, reuse

- Voluntary
- No linking of information
- Intuitive use
- Choice amongst service providers

Identity Ecosystem Participants

- Individual: The person engaged in an online transaction. Individuals are the first priority of this Strategy
- Identity Provider: Enrolls and establishes, maintains, and secures the digital identity associated with a subject.
- Attribute Provider: Asserts trusted, validated attribute claims in response to attribute requests from relying parties.
- Relying Party: Selects and trusts the identity and attribute providers of their choice based on risk and functional requirements.

Identity Ecosystem and Individuals

For individuals, the envisioned Identity Ecosystem is:

- privacy-enhancing
- user-centric
- voluntary

Fair Information Practice Principles

- Multifaceted integration of 8 FIPPs as articulated by DHS
- Example: Data Minimization
    - identity providers
    - relying parties
    - technical standards

Two Parts:

The National Strategy for Trusted Identities in Cyberspace (NSTIC)

- **National Strategy**
- **Signed by the President**

•NSTIC Implementation Plan

- **Detailed activities to support Strategy's vision**
- **Lead Agency assigned to each activity**

Next Steps

- Clear Strategy for Presidential signature
- Conduct next stakeholder review of Implementation Plan
- Establish National Program Office as Federal focal point
- Complete and release Implementation Plan
- Execute Implementation Activities
  - Expand government services, pilots, and policies
  - Address liability
  - Coordinate development of risk models and interop standards
  - Coordinate and enhance international efforts
  - Implement privacy protections
  - More actions to enable the Identity Ecosystem…