NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Privacy Workshop
June 27-28, 2011

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Privacy Workshop
June 27-28, 2011

Jeremy Grant

NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

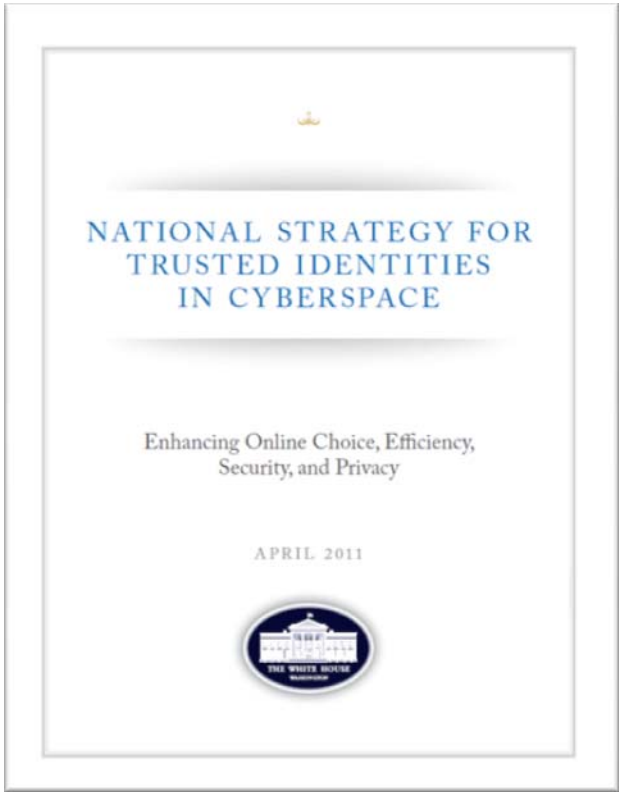
What is NSTIC?

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.”



NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Enhancing Online Choice, Efficiency, Security, and Privacy

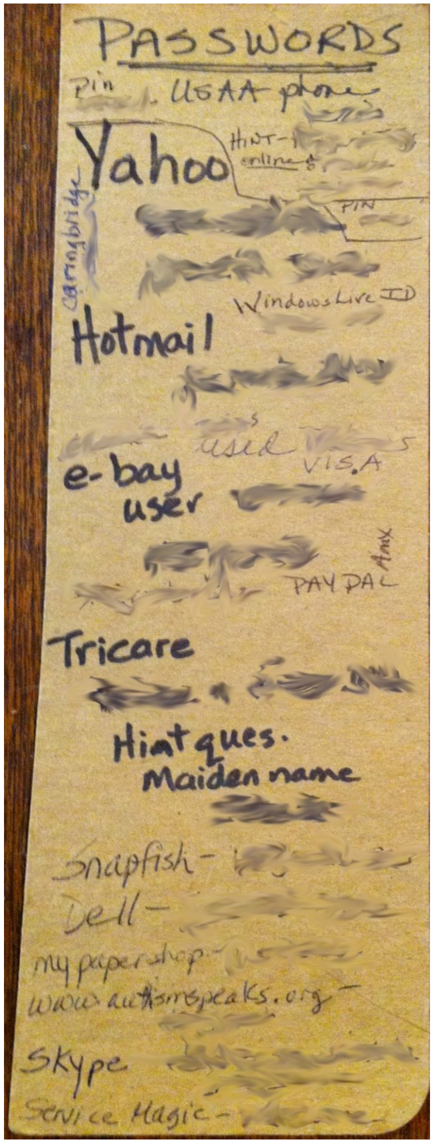
APRIL 2011

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



PASSWORDS

Pin [redacted]. USAA phone [redacted]

Yahoo HINT-[redacted] online [redacted]

[redacted] PIN [redacted]

Caringbridge [redacted]

[redacted]

Windows Live ID [redacted]

Hotmail

[redacted]

[redacted] used [redacted] VISA

e-bay user [redacted]

[redacted] Amx

PAY PAL

Tricare

[redacted]

Hint ques.
Maiden name
[redacted]

Snapfish - [redacted]

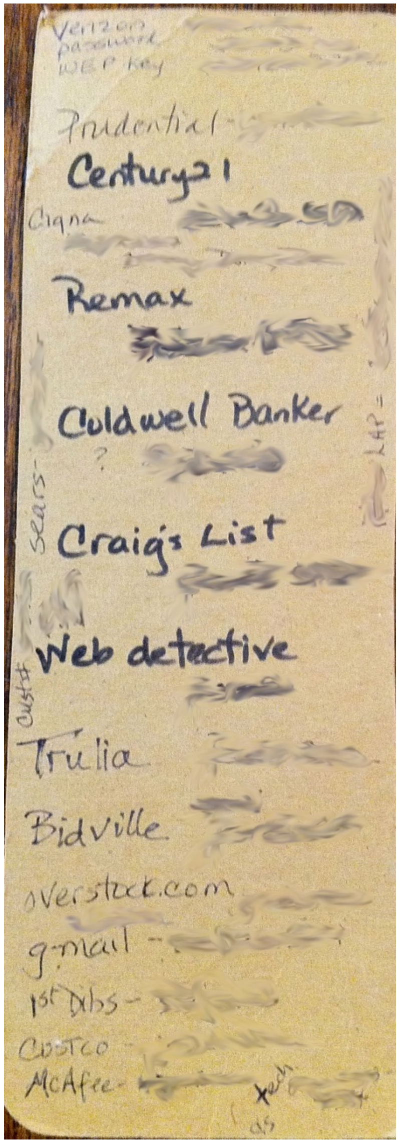
Dell - [redacted]

my papershop - [redacted]

www.autismspeaks.org - [redacted]

Skype [redacted]

Service Magic - [redacted]



Verizon password WEP key [redacted]

Prudential - [redacted]

Century21

Cigna [redacted]

Remax

[redacted]

Coldwell Banker

? [redacted]

LHP = [redacted]

Sears - [redacted]

Craig's List [redacted]

Cust# [redacted]

Web detective [redacted]

Trulia [redacted]

Bidville [redacted]

overstock.com [redacted]

g-mail - [redacted]

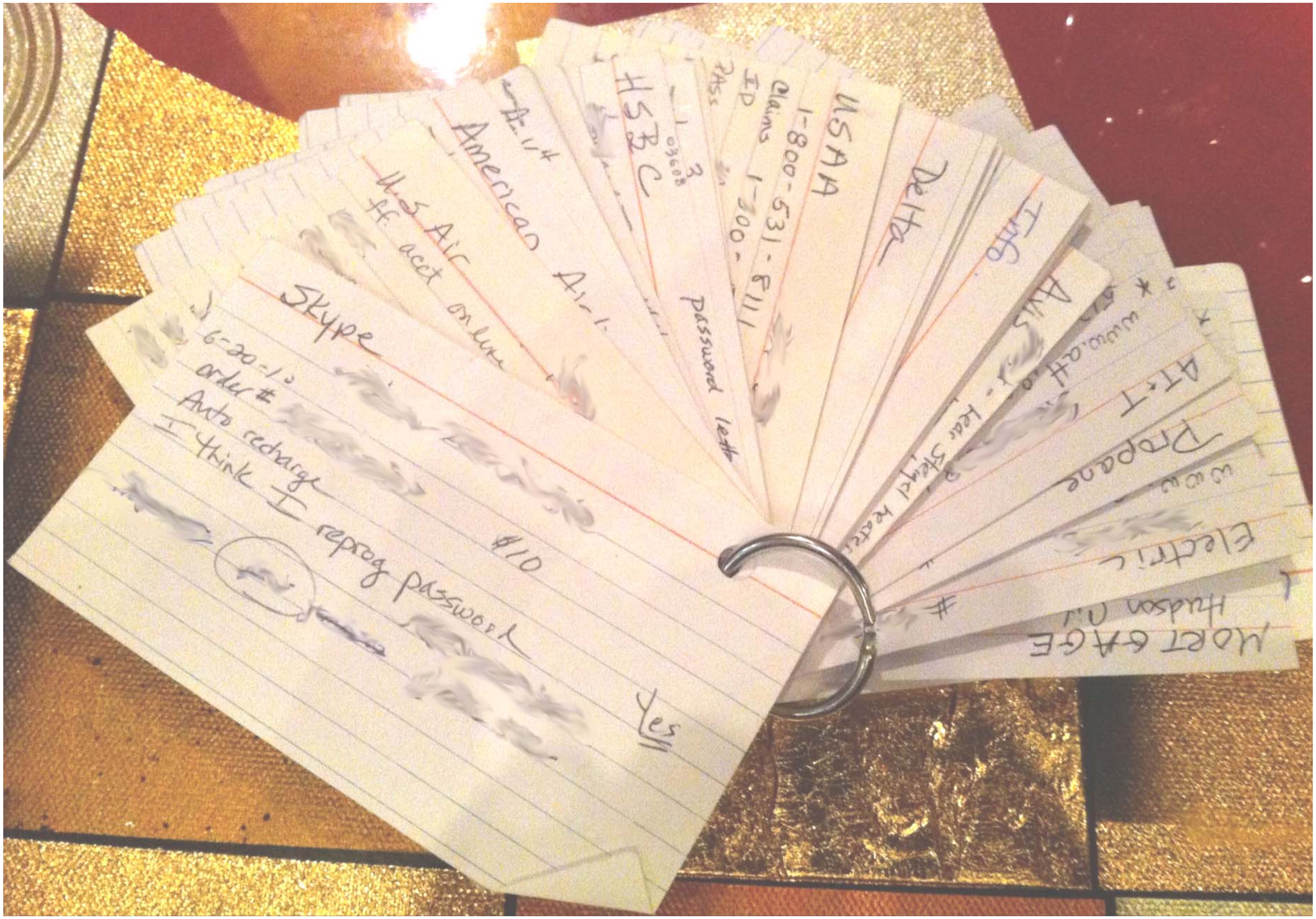
1st Dibs - [redacted]

Costco - [redacted]

McAfee - [redacted] x each [redacted]

ds

There’s a Problem Today, Travel Edition

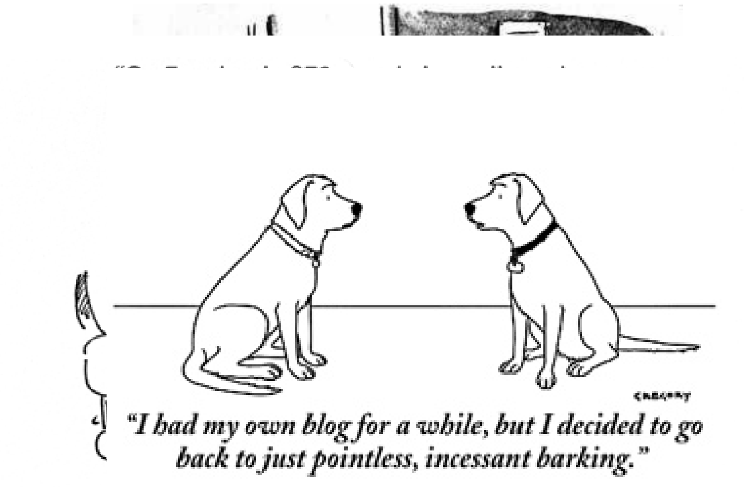


The Problem Today

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, 2007

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

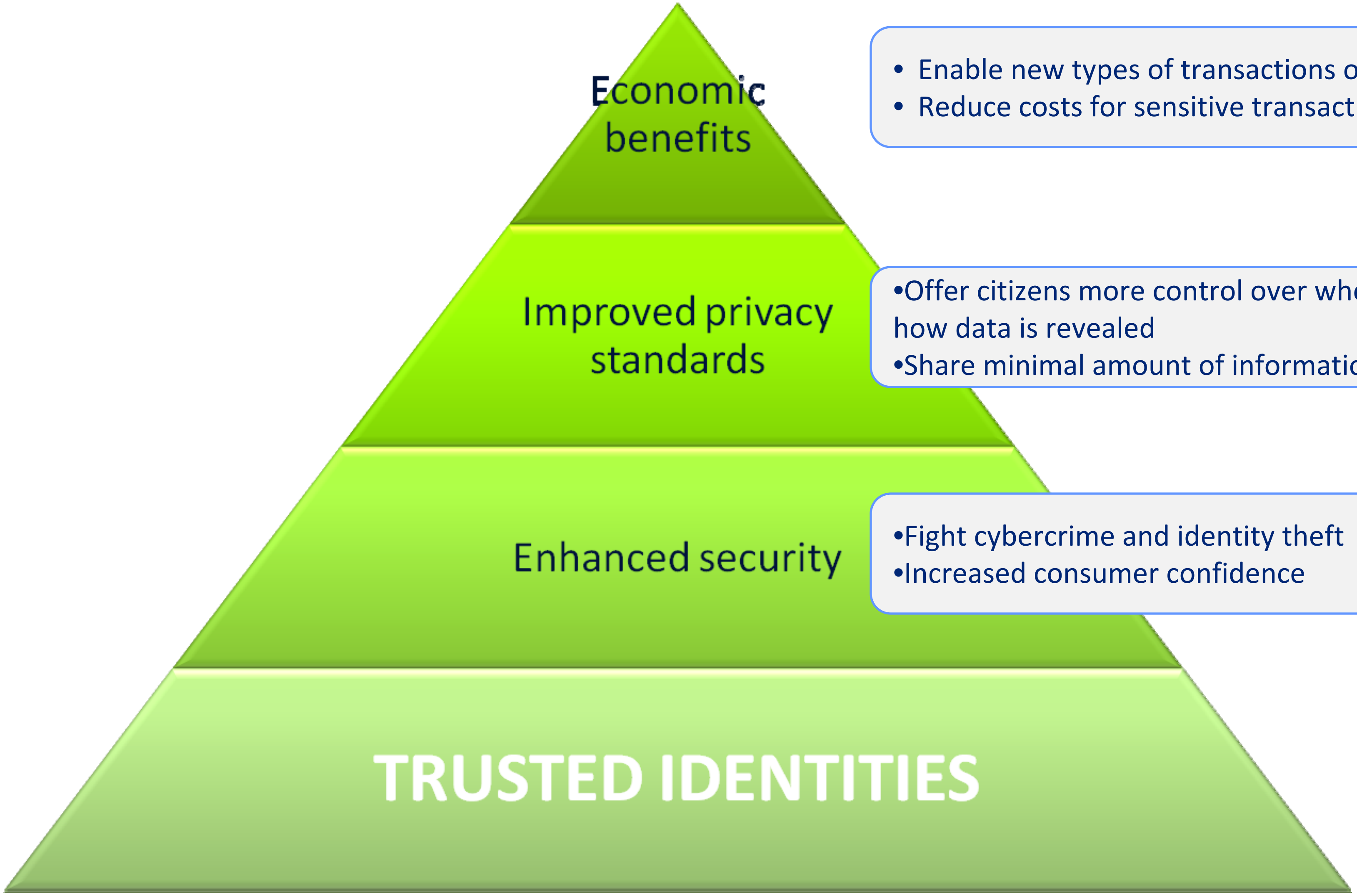
The Problem Today

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
Commissioner of Motor Vehicles
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
8AJ120T521
Sample License Document

Trusted Identities provide a foundation



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

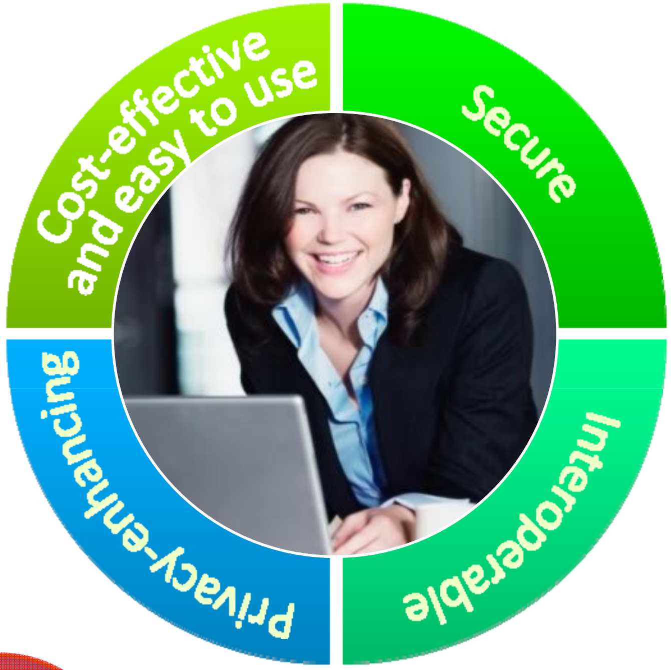
•Offer citizens more control over when and how data is revealed
•Share minimal amount of information

•Fight 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.

Apply for mortgage online with e-signature

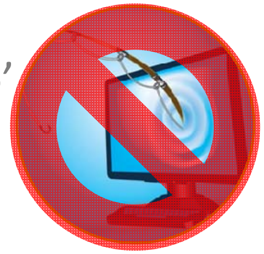


Online shopping with minimal sharing of PII

Trustworthy critical service delivery

Secure Sign-On to state website

Security 'built-into' system to reduce user error



Privately post location to her friends

NSTIC Guiding Principles

Identity Solutions will be:

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

We've proven that Trusted Identities matter

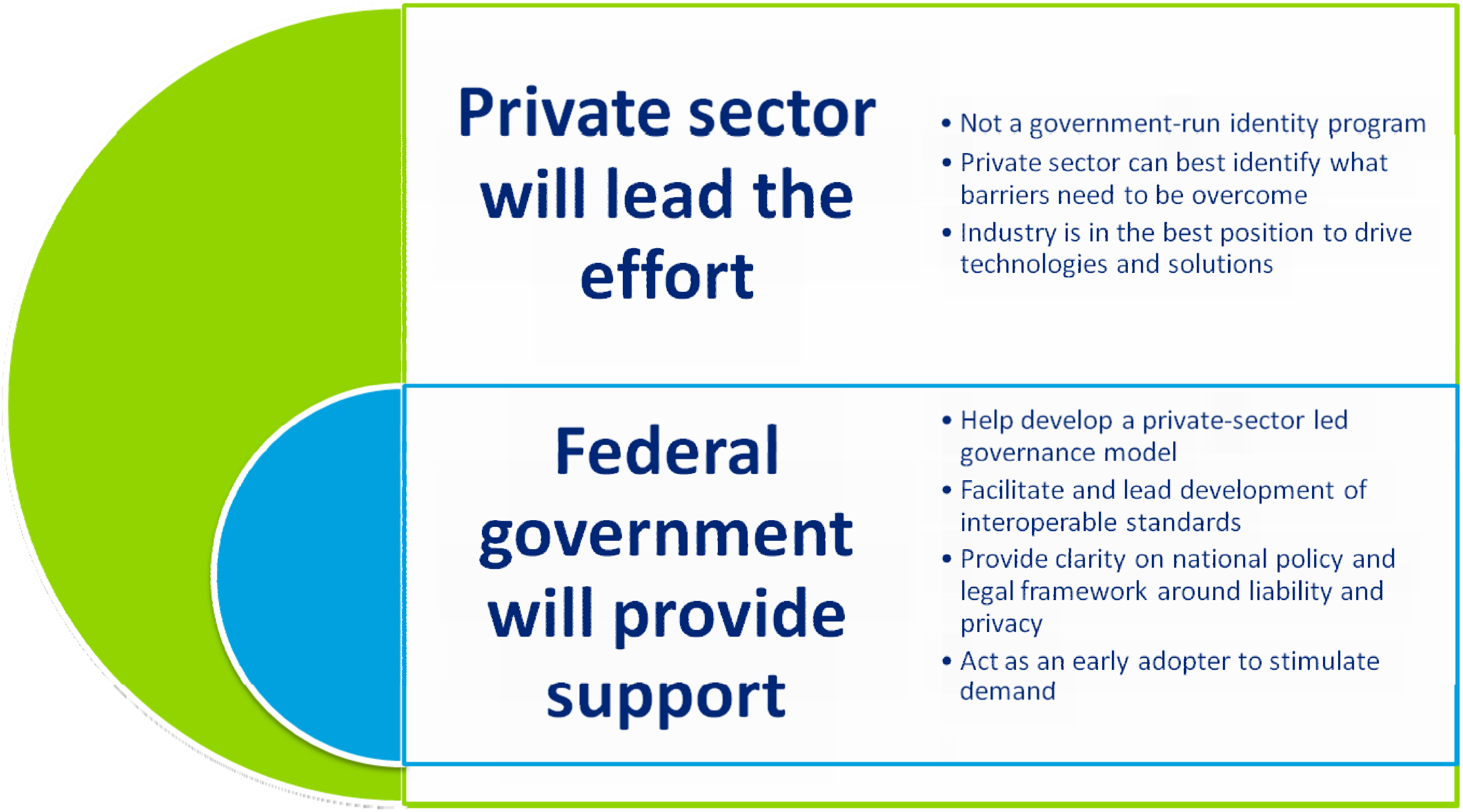
DoD Led the Way

- 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
- Private sector can best identify what barriers need to be overcome
- Industry is in the best position to drive technologies and solutions

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

NSTIC: The specifics…

"Giving consumers choices for solving these kinds of problems is at the heart of this new strategy. And it is one that relies not on government, but on the private sector, to design the technologies and tools that will help make our identities more secure in cyberspace and to make those tools available to consumers who want them. It asks companies to pursue these solutions in ways that will not impinge on the vitality and dynamism of the web, or force anyone to give up the anonymity they enjoy on the Internet."

NSTIC: The specifics…

NSTIC Goal 1 (p. 29):

Develop a comprehensive Identity Ecosystem Framework.

“The Identity Ecosystem Framework is the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that govern the Identity Ecosystem.

“It will guide the development of individual trust frameworks and will be flexible enough to accommodate the varied needs of Identity Ecosystem participants.”

The Identity Ecosystem Framework

- The Steering Group to develop the Identity Ecosystem Framework must enable a true public-private partnership.

- Its objective: to take the lead in convening stakeholders from all sectors to figure out how to develop policy and technical standards necessary to create the Identity Ecosystem.

- Government will participate in this group and support it – but that does not mean we will lead it.

Federal government will support the private sector…

Role of the Federal Government (p. 37)

•Advocate for and protect individuals;

•Support the private sector's development and adoption of the Identity Ecosystem;

•Partner with the private sector to ensure that the Identity Ecosystem is sufficiently interoperable, secure, and privacy protecting;

•Provide and accept Identity Ecosystem services for which it is uniquely suited; and

•Lead by example and implement the Identity Ecosystem for the services it provides internally and externally.

The NSTIC Governance Notice of Inquiry (NOI)

Released June 8, 2011

- Objective: to seek comments on the requirements of, and possible models for, the NSTIC steering group

- Focus on 4 key issues:
  1. Steering Group Structure
  2. Steering Group Initiation
  3. Representation of Stakeholders
  4. International Considerations

- Comments are due on or before July 22, 2011

The NSTIC Governance NOI

What we hope to gain from it

- Ideas and recommendations
- Lessons learned from other efforts
- Meaningful input from a wide array of stakeholders

What we will do with it/how we will respond

- Inputs will inform our deliberations and decisions on the steering body; all comments will be analyzed
- All submissions will be part of the public record
- NIST will produce a public report with recommendations for addressing, at a minimum, questions raised on the four key issues

NSTIC: Privacy is Paramount

Executive Summary

“The enhancement of privacy and support of civil liberties is a guiding principle of the envisioned Identity Ecosystem.

“The Identity Ecosystem will use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual’s transactions, thus ensuring that no one service provider can gain a complete picture of an individual’s life in cyberspace. By default, only the minimum necessary information will be shared in a transaction. For example, the Identity Ecosystem will allow a consumer to provide her age during a transaction without also providing her birth date, name, address, or other identifying data.

“In addition to privacy protections, the Identity Ecosystem will preserve online anonymity and pseudonymity, including anonymous browsing. These efforts to enhance privacy and otherwise support civil liberties will be part of, and informed by, broader privacy policy development efforts occurring throughout the Administration.

“Equally important, participation in the Identity Ecosystem will be voluntary: the government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them.”

Guiding Principle #1: Identity Solutions will be Privacy-Enhancing and Voluntary

“Ideally, identity solutions should preserve the positive privacy benefits of offline transactions while mitigating some of the negative privacy aspects.

“The Fair Information Practice Principles (FIPPs) are the widely accepted framework for evaluating and mitigating privacy impacts.”

Guiding Principle #1: Identity Solutions will be Privacy-Enhancing and Voluntary

Fair Information Practice Principles (FIPPs)

1.**Transparency:** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).

2.**Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

3.**Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

4.**Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Guiding Principle #1: Identity Solutions will be Privacy-Enhancing and Voluntary

Fair Information Practice Principles (FIPPs)

5.Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

6.Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

7.Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8.Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Guiding Principle #1: Identity Solutions will be Privacy-Enhancing and Voluntary.

“The envisioned Identity Ecosystem will be grounded in a holistic implementation of the FIPPs in order to provide multi-faceted privacy protections. For example, organizations will collect and distribute only the information necessary to the transaction, maintain appropriate safeguards on that information, and be responsive and accountable to individuals’ privacy expectations. In circumstances where individuals make choices regarding the use of their data (such as to restrict particular uses), those choices will be automatically applied to all parties with whom that individual interacts.

“Consistent with the FIPPs-based approach, the Identity Ecosystem will include limits on the length of time organizations can retain personal information and will require them to provide individuals with appropriate opportunities to access, correct, and delete it. The Identity Ecosystem will also require organizations to maintain auditable records regarding the use and protection of personal information.”

Guiding Principle #1: Identity Solutions will be Privacy-Enhancing and Voluntary.

“Moreover, a FIPPs-based approach will promote the creation and adoption of privacy-enhancing technical standards. Such standards will minimize the transmission of unnecessary information and eliminate the superfluous “leakage” of information that can be invisibly collected by third parties. Such standards will also minimize the ability to link credential use among multiple service providers, thereby preventing them from developing a complete picture of an individual’s activities online.

“Finally, service providers will request individuals’ credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction. As a result, implementation of the FIPPs will protect individuals’ capacity to engage anonymously in cyberspace. Universal adoption of the FIPPs in the envisioned Identity Ecosystem will enable a variety of transactions, including anonymous, anonymous with validated attributes, pseudonymous, and uniquely identified—while providing robust privacy protections that promote usability and trust.”

Guiding Principle #1: Identity Solutions will be Privacy-Enhancing and Voluntary.

“Finally, participation in the Identity Ecosystem will be voluntary: the government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them.

“Individuals shall be free to use an Identity Ecosystem credential of their choice, provided the credential meets the minimum risk requirements of the relying party, or to use any non-Identity Ecosystem mechanism provided by the relying party. Individuals’ participation in the Identity Ecosystem will be a day-to-day—or even a transaction-to-transaction—choice.”

Objective 1.1: Establish improved privacy protection mechanisms

“The Identity Ecosystem Framework must offer individuals better means of protecting their privacy by establishing clear rules and guidelines based upon the FIPPs.

“These rules and guidelines must address not only the circumstances under which a service provider or relying party may share information but also the kinds of information that they may collect and how that information is used. New privacy protections will shift the current model of application-specific collection of identity information to a distributed, user-centric model that supports an individual’s capability to manage an array of cyber identities and to manage and assert personal attributes without having to provide identifying data. The new model will reduce the number of service providers with whom individuals must share their personal information in the course of everyday transactions.”

Objective 1.1: Establish improved privacy protection mechanisms

The Executive Branch of the Federal Government will work with the private sector and, if necessary, propose legislation to strengthen privacy protections for individuals. These protections will enable individuals to form consistent expectations about the treatment of their information in cyberspace.

Although individuals will retain the right to exchange their personal information in return for services they value, these protections will ensure that the default behavior of Identity Ecosystem providers is to:

•Limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements;

•Limit the use of the individual's data that is collected and transmitted to specified purposes;

Objective 1.1: Establish improved privacy protection mechanisms (cont'd.)

- Limit the retention of data to the time necessary for providing and administering the services to the individual end-user for which the data was collected, except as otherwise required by law;

- Provide concise, meaningful, timely, and easy-to-understand notice to end-users on how providers collect, use, disseminate, and maintain personal information;

- Minimize data aggregation and linkages across transactions;

- Provide appropriate mechanisms to allow individuals to access, correct, and delete personal information;

Objective 1.1: Establish improved privacy protection mechanisms (cont'd.)

- Establish accuracy standards for data used in identity assurance solutions;

- Protect, transfer at the individual's request, and securely destroy information when terminating business operations or overall participation in the Identity Ecosystem;

- Be accountable for how information is actually used and provide mechanisms for compliance, audit, and verification; and

- Provide effective redress mechanisms for, and advocacy on behalf of, individuals who believe their data may have been misused.

White House Perspectives

Naomi Lefkovitz

National Security Staff
Executive Office of the President

How the workshop will proceed

Two Panels

- Today: Privacy in Practice: A Case Study and Discussion on Implementing the FIPPs in the Identity Ecosystem
- Tomorrow: Privacy-Enhancing Technologies, Usability and the End-User Experience

Three breakout sessions

- Two today 1:15-4:30pm ; One tomorrow 10:45-12:15
- Attendees can participate in whichever sessions they like
- Day 1 breakout summaries this afternoon; Day 2 after lunch tomorrow
- Lunch on your own both days

Keep in mind…

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

Identity Solutions will be:

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