National Strategy for Trusted Identities in Cyberspace

VCAT Discussion | 2.8.2012

Jeremy Grant

NIST

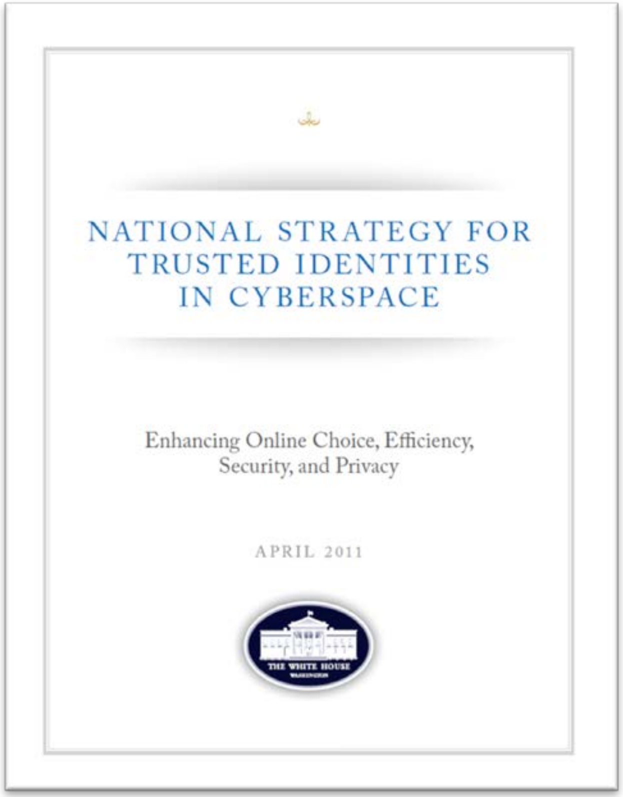
What is NSTIC?

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.”



NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Enhancing Online Choice, Efficiency, Security, and Privacy

APRIL 2011

THE WHITE HOUSE

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
  - 8.1M U.S. victims in 2010 at a cost of $37 billion (Javelin)
- A common vector of attack
  - Sony Playstation, Zappos, Lulzsec, Infragard among dozens of 2011-12 breaches tied to passwords.

The Problem Today

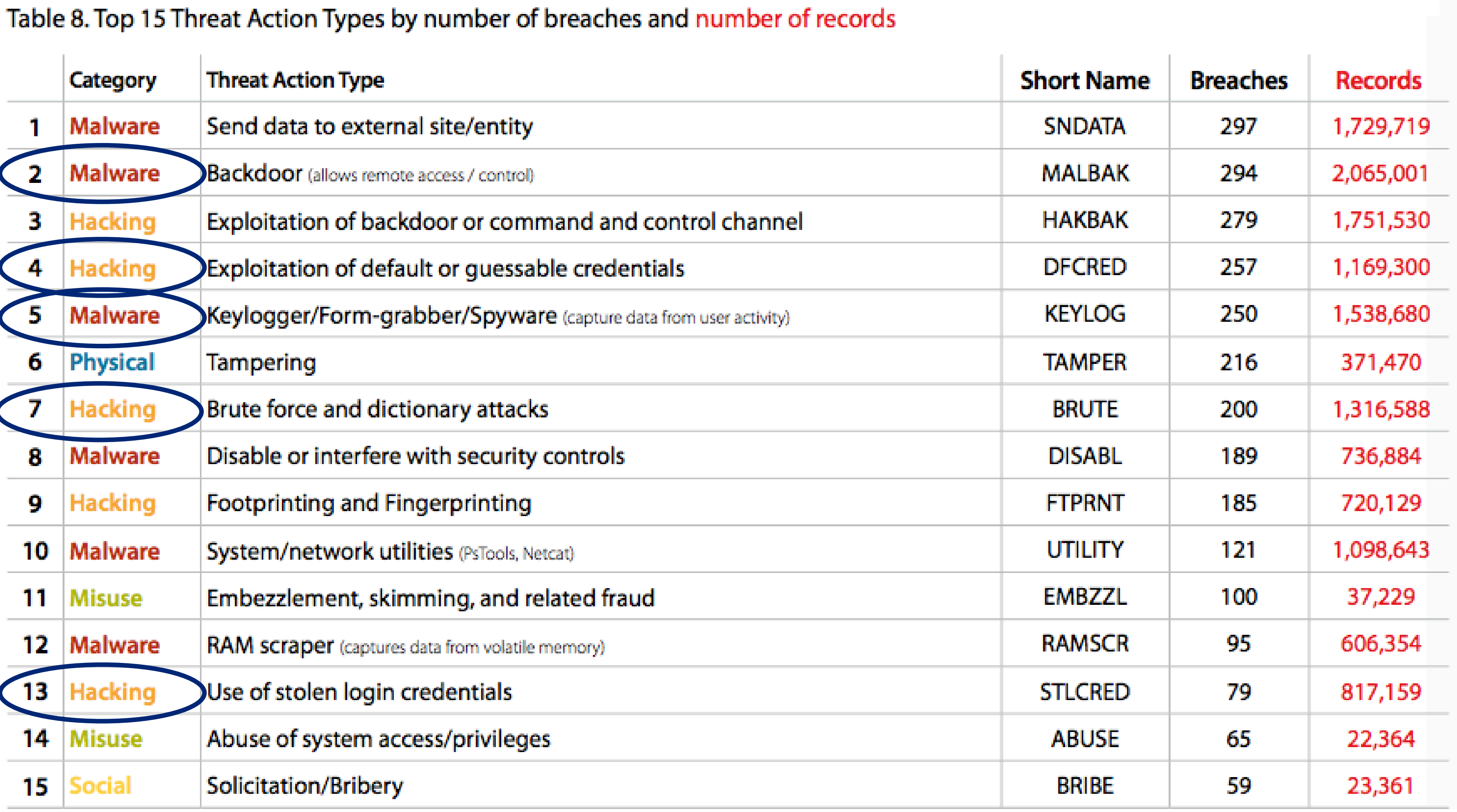


Table 8. Top 15 Threat Action Types by number of breaches and number of records

	Category	Threat Action Type	Short Name	Breaches	Records
1	Malware	Send data to external site/entity	SNDATA	297	1,729,719
2	Malware	Backdoor (allows remote access / control)	MALBAK	294	2,065,001
3	Hacking	Exploitation of backdoor or command and control channel	HAKBAK	279	1,751,530
4	Hacking	Exploitation of default or guessable credentials	DFCRED	257	1,169,300
5	Malware	Keylogger/Form-grabber/Spyware (capture data from user activity)	KEYLOG	250	1,538,680
6	Physical	Tampering	TAMPER	216	371,470
7	Hacking	Brute force and dictionary attacks	BRUTE	200	1,316,588
8	Malware	Disable or interfere with security controls	DISABL	189	736,884
9	Hacking	Footprinting and Fingerprinting	FTPRNT	185	720,129
10	Malware	System/network utilities (PsTools, Netcat)	UTILITY	121	1,098,643
11	Misuse	Embezzlement, skimming, and related fraud	EMBZZL	100	37,229
12	Malware	RAM scraper (captures data from volatile memory)	RAMSCR	95	606,354
13	Hacking	Use of stolen login credentials	STLCRED	79	817,159
14	Misuse	Abuse of system access/privileges	ABUSE	65	22,364
15	Social	Solicitation/Bribery	BRIBE	59	23,361

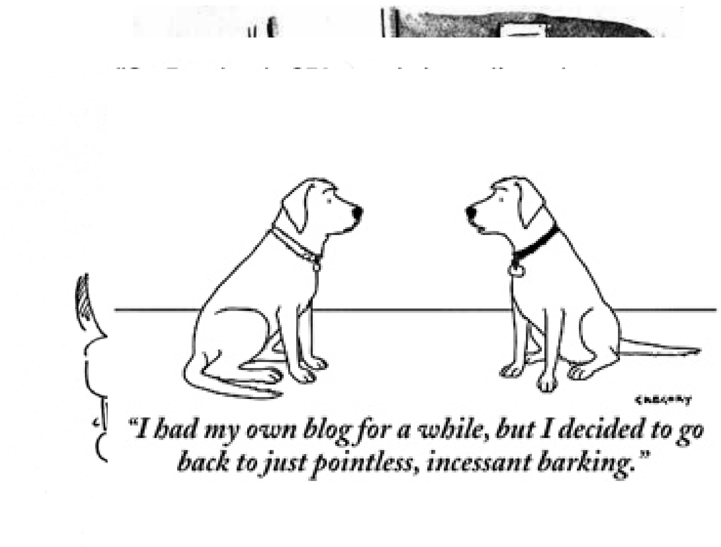
Source: 2011 Data Breach Investigations Report, Verizon and USSS

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, September 19, 2005
Rob Cottingham, July 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

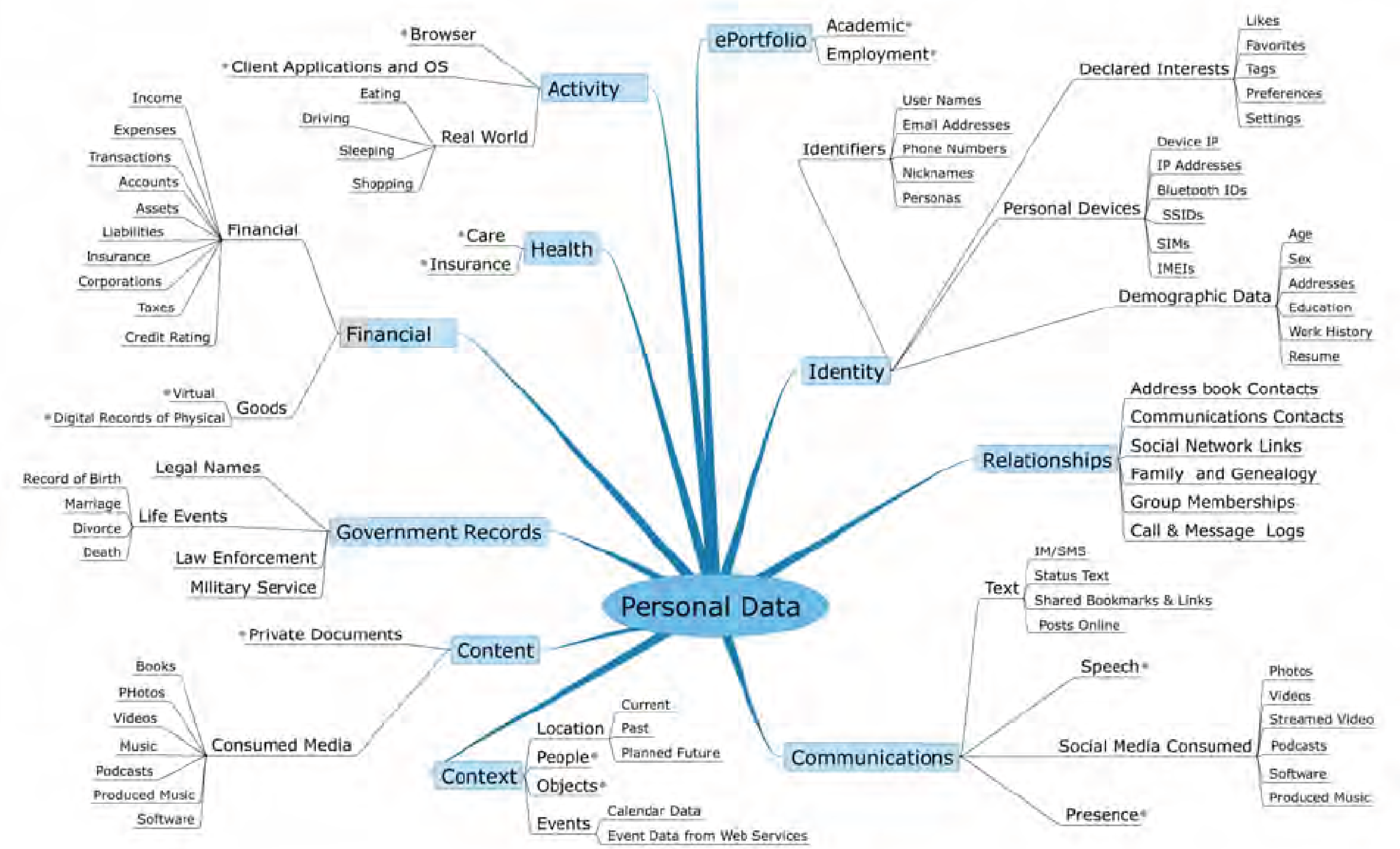
Privacy remains a challenge

- 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

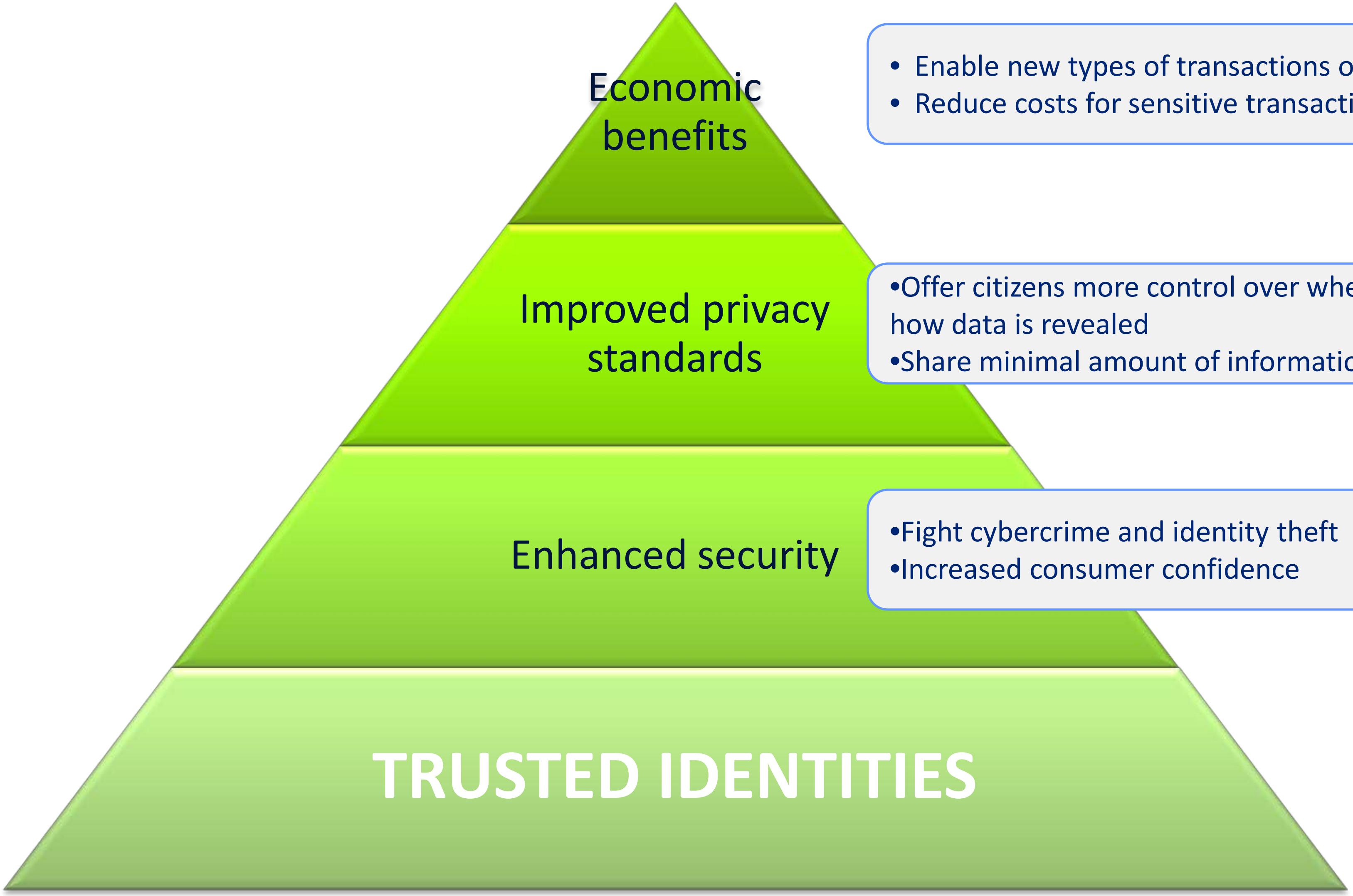
NEW YORK STATE
Commissioner of Motor Vehicles
ENHANCED
DRIVER LICENSE
ID: 012 345 678
CLASS D
DOCUMENT
SAMPLE, LICENSE
2345 ANYPLACE AVE
ANYTOWN NY 12345
DOB: 06-09-85
SEX: F EYES: BR HT: 5-09
E: NONE
R: NONE
ISSUED: 09-30-08 EXPIRES: 10-01-16
8AJ120T521
Sample License Document

Personal Data is Abundant…and Growing



Source of data types from the Rethinking Personal Data Pre-Read Document published by the World Economic Forum written by Marc Davis et al published in June, 2010.

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

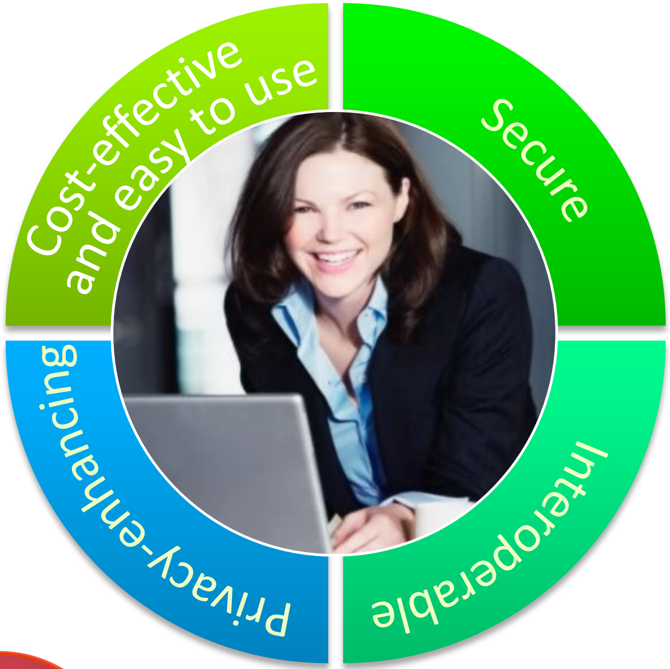
•Fight cybercrime and identity theft

•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

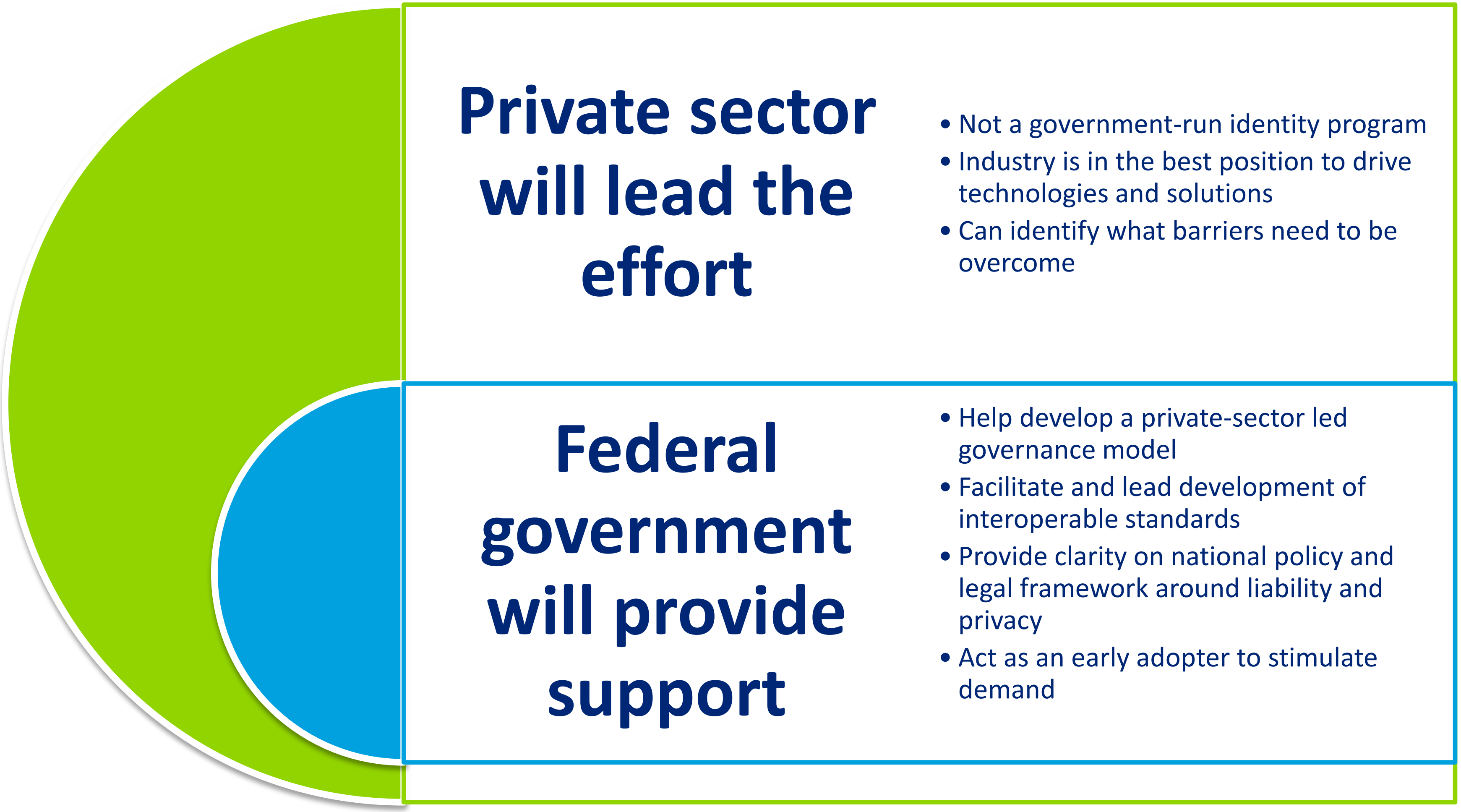
Trustworthy critical service delivery

Secure Sign-On to state website

Security ‘built-into’ system to reduce user error

Privately post location to her friends

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

NSTIC National Program Office

- Charged with leading day-to-day coordination across government and the private sector in implementing NSTIC
- Funded with $16.5M for FY12

Key 2012 NSTIC Implementation Activities

1. Establishment of the Identity Ecosystem Steering Group
   - NIST Recommendations to be published mid-February
   - New 2-year grant to fund a privately-led (.com or .org) Steering Group to convene stakeholders and craft standards and policies to create an Identity Ecosystem Framework

2. NSTIC Pilots Grant Program
   - FFO recently published for $10M NSTIC pilots grant program
   - 5-8 awards expected by late summer
   - Focus on addressing barriers the marketplace has not yet overcome

     "Make something happen that otherwise would not"

Key 2012 NSTIC Implementation Activities

3. Buildout of NPO
   - Hire key staff (tech, privacy, governance, pilots leads)
   - Model: influence via active engagement in Steering Group and managing pilots

4. Coordinate Federal efforts for .gov adoption
   - Government agency embrace of NSTIC is key to convincing non-governmental stakeholders that the Strategy is viable
   - Identifying agencies with potential killer apps and willingness to be early adopters

We've proven that Trusted Identities matter

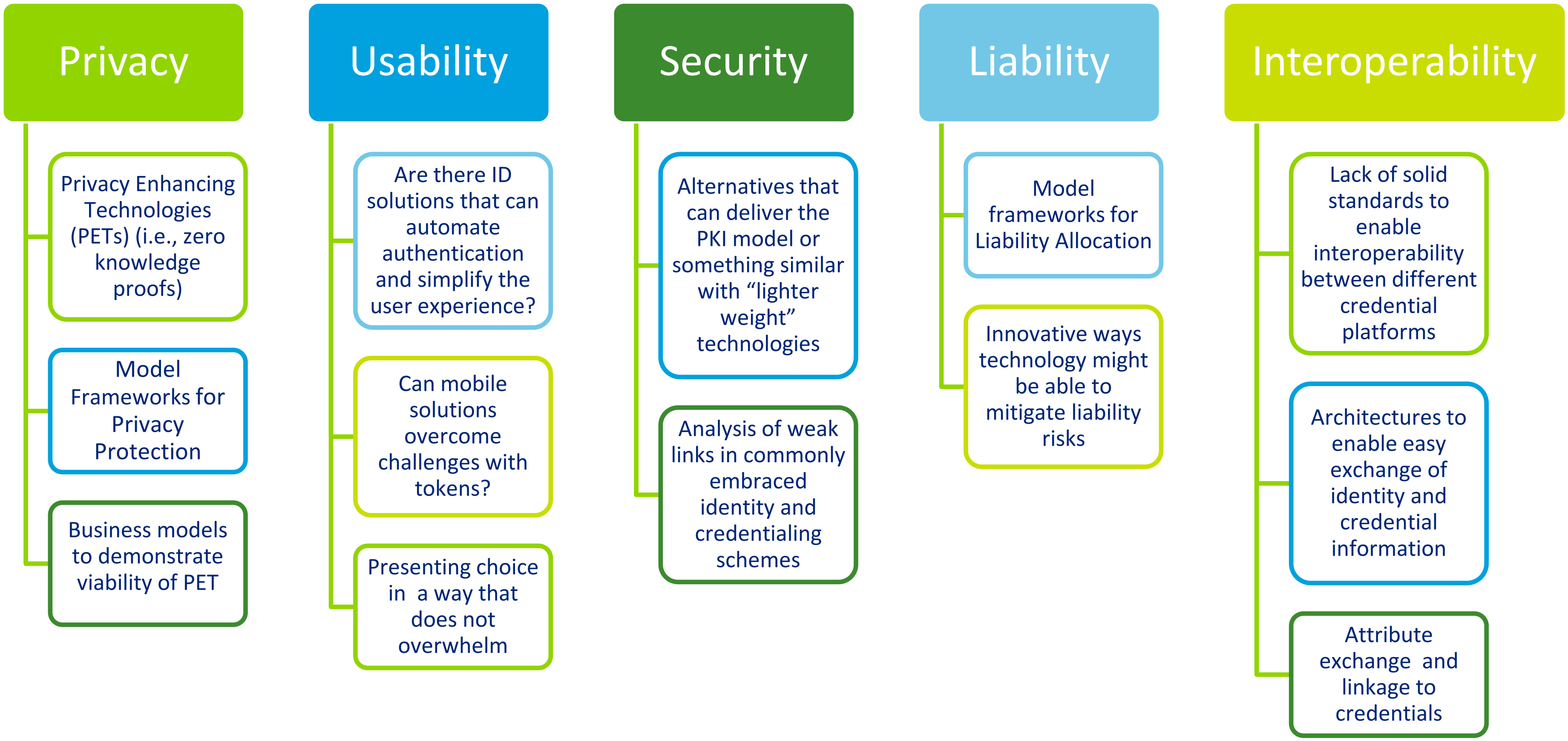
DoD Led the Way

- 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.

Barriers help guide where Pilots, R&D are needed



Privacy

- Privacy Enhancing Technologies (PETs) (i.e., zero knowledge proofs)
- Model Frameworks for Privacy Protection
- Business models to demonstrate viability of PET

Usability

- Are there ID solutions that can automate authentication and simplify the user experience?
- Can mobile solutions overcome challenges with tokens?
- Presenting choice in a way that does not overwhelm

Security

- Alternatives that can deliver the PKI model or something similar with “lighter weight” technologies
- Analysis of weak links in commonly embraced identity and credentialing schemes

Liability

- Model frameworks for Liability Allocation
- Innovative ways technology might be able to mitigate liability risks

Interoperability

- Lack of solid standards to enable interoperability between different credential platforms
- Architectures to enable easy exchange of identity and credential information
- Attribute exchange and linkage to credentials

Questions?

Jeremy Grant

jgrant@nist.gov

202.482.3050