

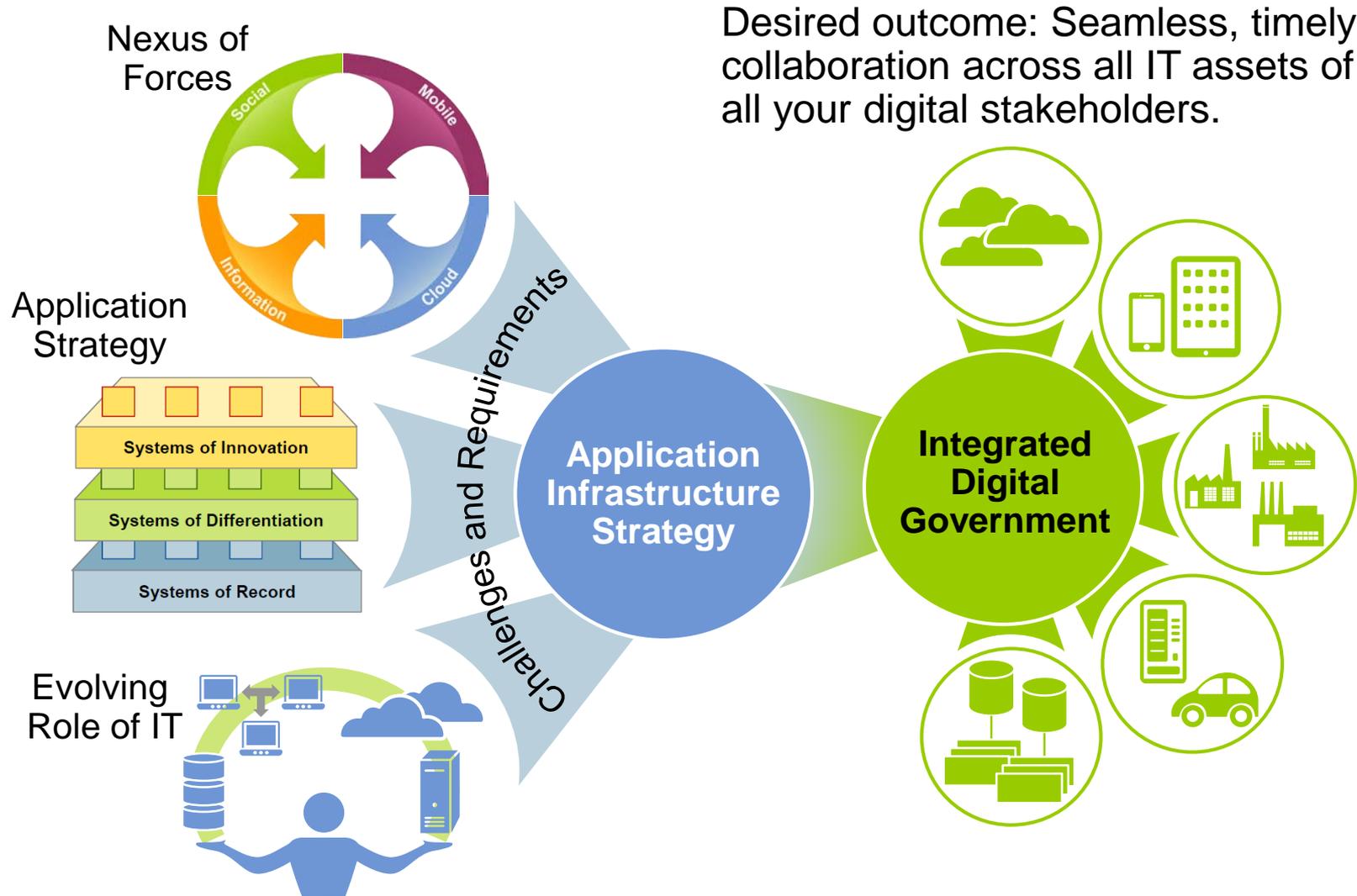
# What Does the National Strategy for Trusted Identities in Cyberspace Mean to the Digital Transformation of Society

Jeff Vining

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](#) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."

**Gartner**<sup>®</sup>

# The Goal of the Digital Society Integrated Digital Services



# Key Issues

---

- Why Digital Government?
- What Is NSTIC?
- How Will NSTIC Further Digital Government Service Delivery?

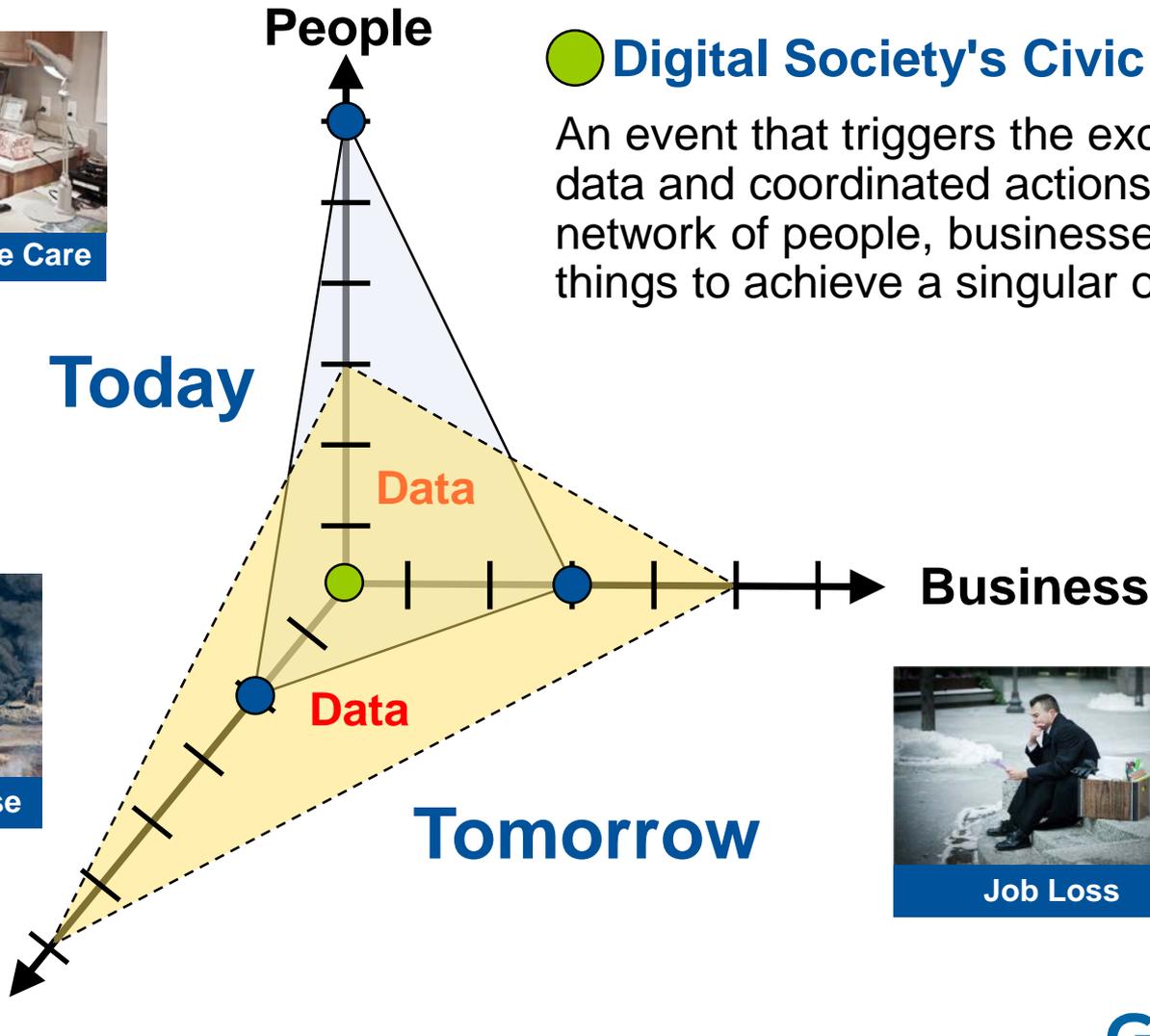
# Government Reflects Society Which Is Result of the Internet of Everything



Elderly Home Care



Emergency Response



## ● Digital Society's Civic Moment

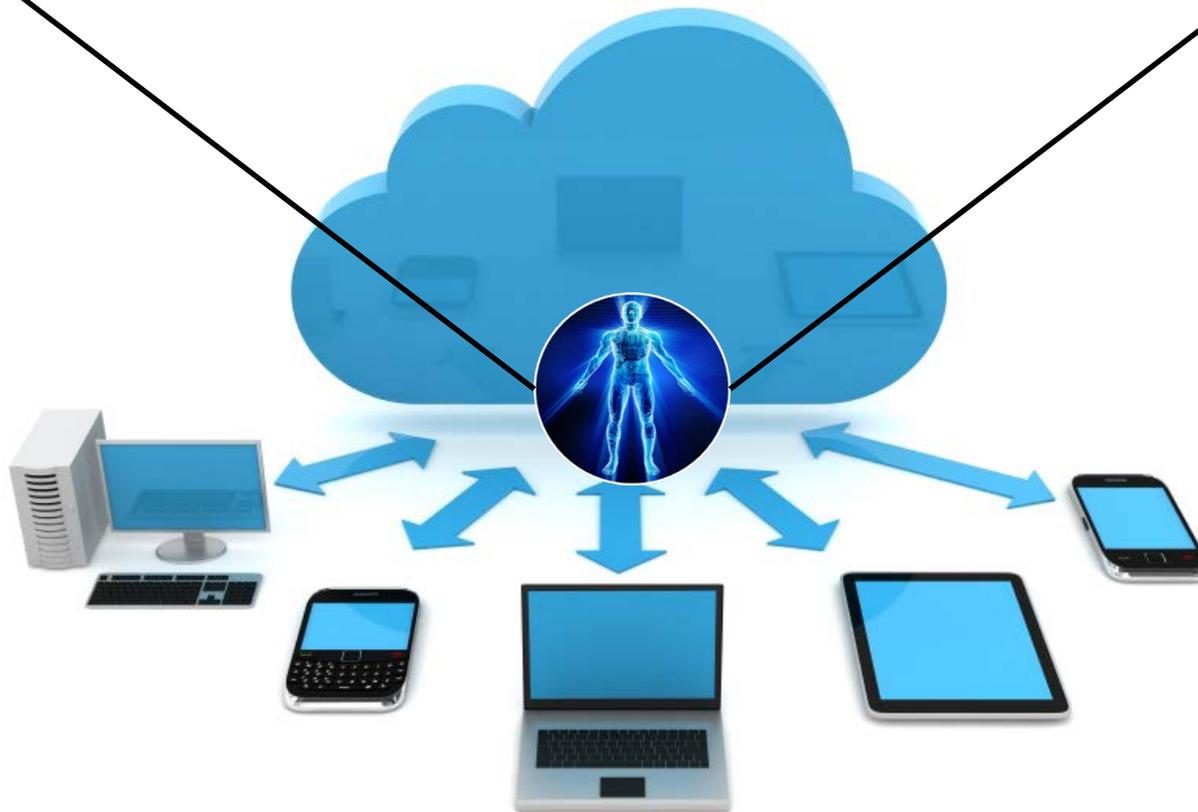
An event that triggers the exchange of data and coordinated actions across a network of people, businesses and things to achieve a singular objective.



Job Loss

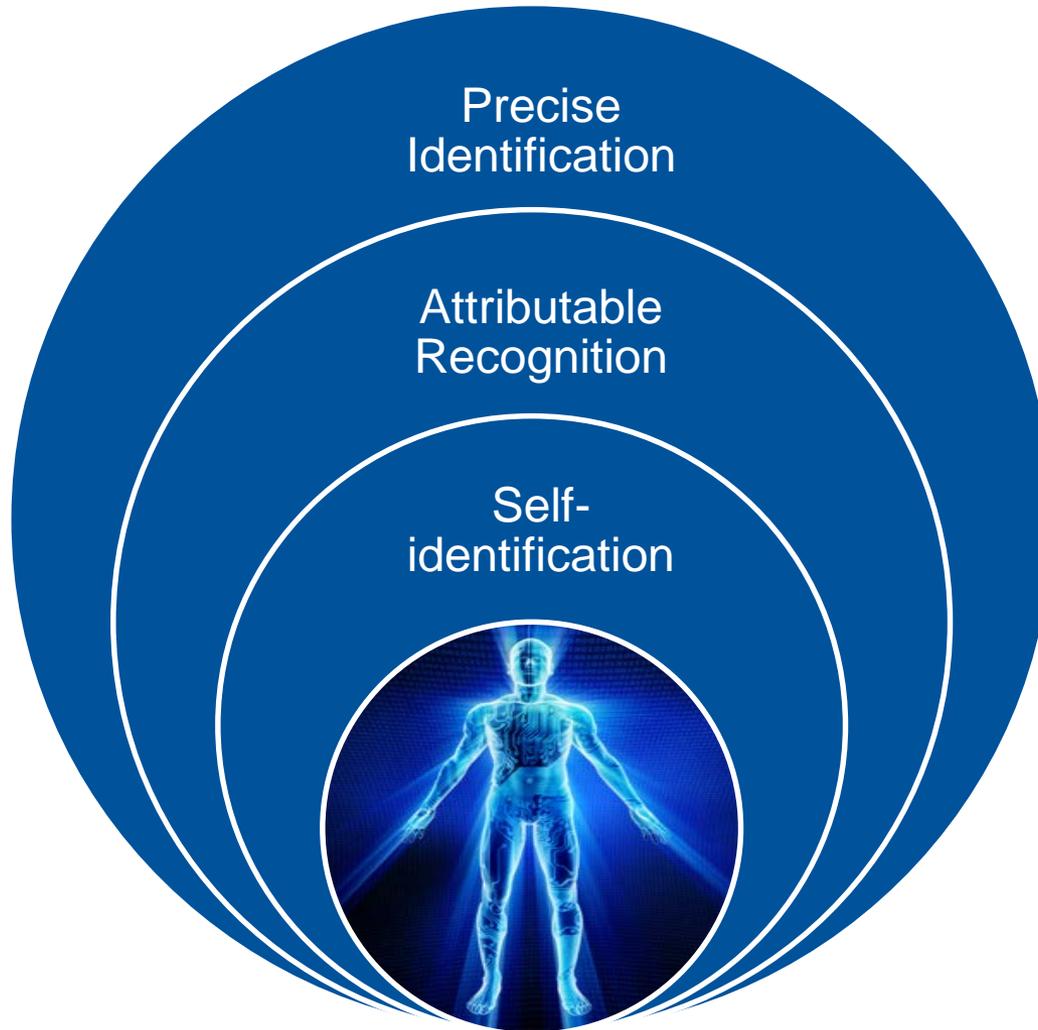
# Identity Core to Digital Government?

Identity is composed of biometric, biographical, attribute and profile information stored and transmitted in digital form enabled and enforced by federated and authentication systems.

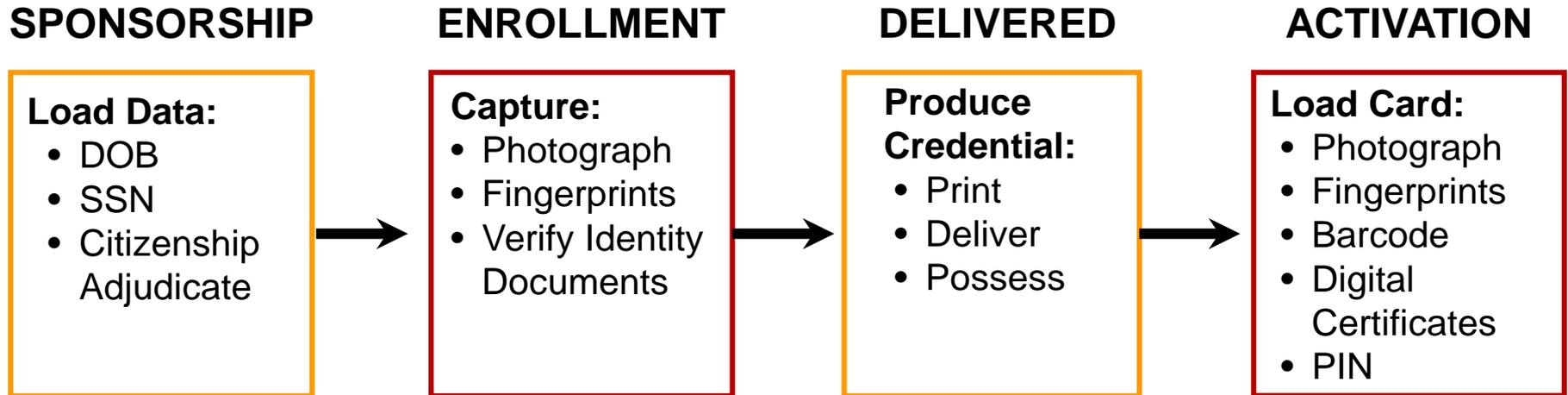


# Identity: It Is the New "You"

---



# Why Is NSTIC Needed?



**Time to receive card — approximately  
2 hours to 2 weeks.**

# Key Issues

---

- Why Digital Government?
- What Is NSTIC?
- How Will NSTIC Further Digital Government Service Delivery?

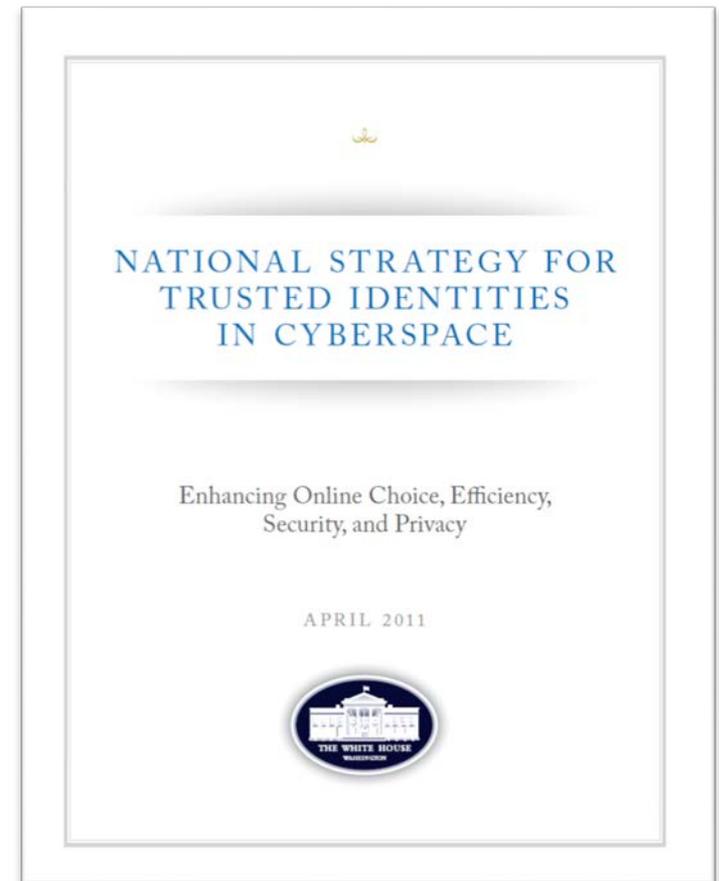
# What Is NSTIC?

A "cybersecurity focused identity management vision and strategy."

## 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."



# NSTIC: Building a Future?

---

## 1 Communities of Trust Forms the Basis:

- Low Risk Establishes Technical Proficiency
- Bottom-up Approach Secures Buy-in

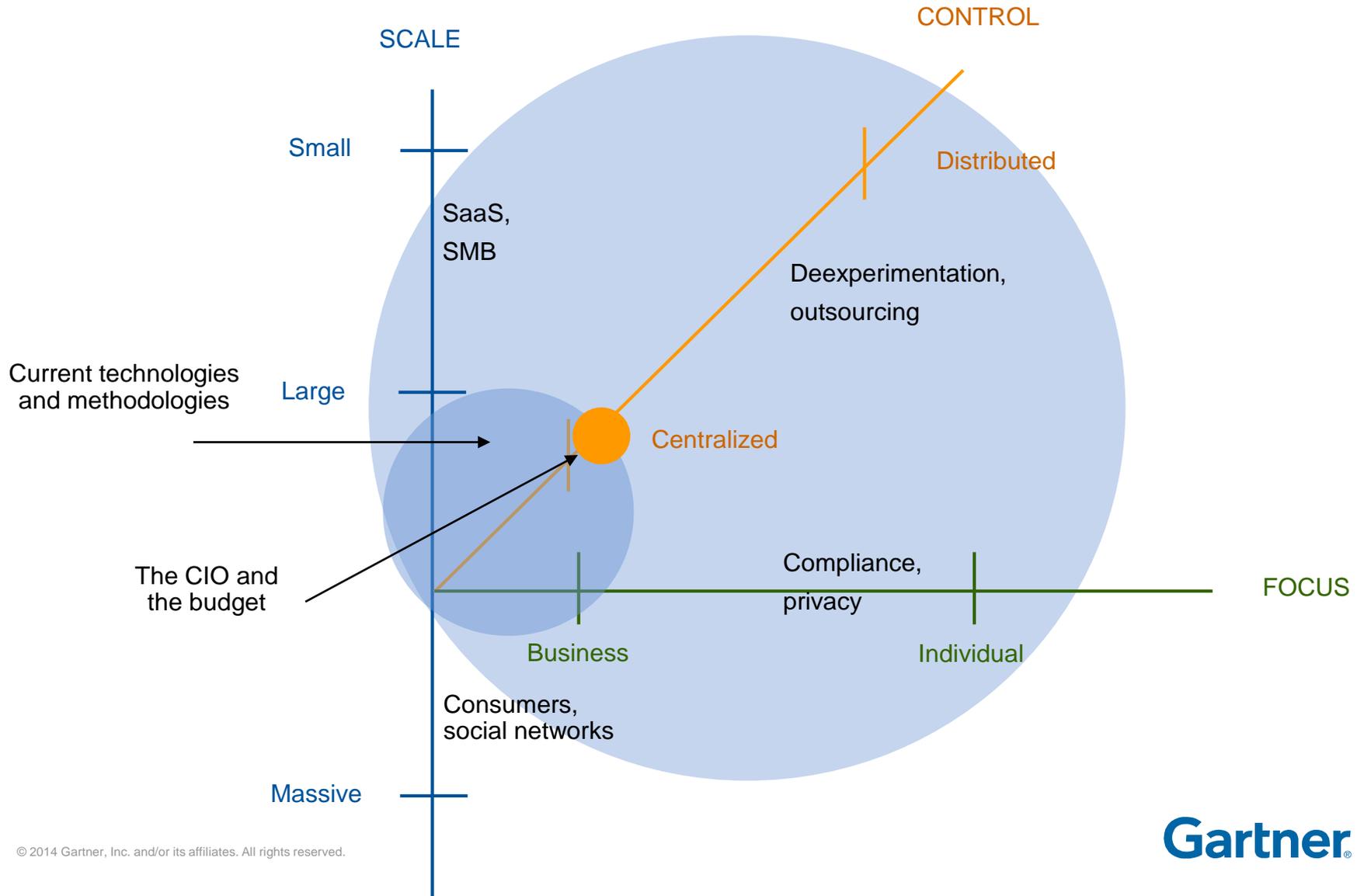
## 2 Extending Communities of Trust Attracts Ecosystem:

- Government Is More Biased Against Federation Than Commercial
- Interagency Cost-effectiveness and Increased Citizen Uptake for E-Services

## 3 Identity Ecosystem:

- Government to Commercial Federations

# Expanding Identity Universe



# Moving Toward More of a Digital Service Delivery

---

PC, USB Card Readers  
or Mobile Devices  
Access Portals  
and Applications

## **Government:**

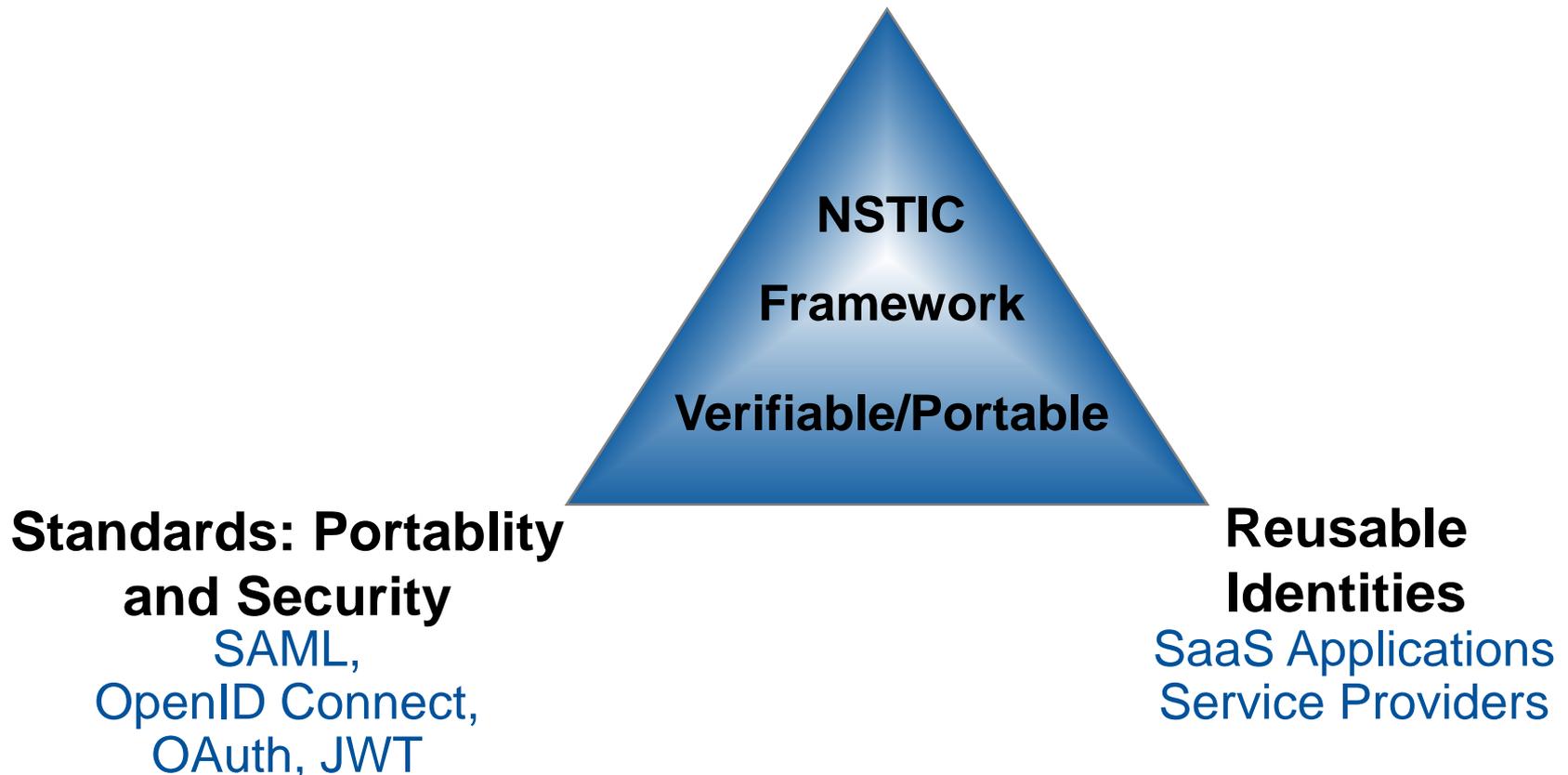
- Education (curriculum, enrollment, fees and registration)
- Healthcare (appointments, benefits, claims, locations and physicians)
- Payments (paying account balances, fines, parking, property assessments, transportation services, utility bills and taxes)
- Citizenship (registration and online voting, and immigration and passport services)
- Reporting emergency and nonemergency events
- Human welfare (applying for and monitoring social welfare benefits, searching for child care centers or submitting housing offers)

# NSTIC: Trust, Standards, Portability and Collaboration

---

## Trust Frameworks: Adoption by Private Sector

Foster Competitive Development of  
Stronger Identity Proofing Standards



# Key Issues

---

- Why Digital Government?
- What Is NSTIC?
- How Will NSTIC Further Digital Government Service Delivery?

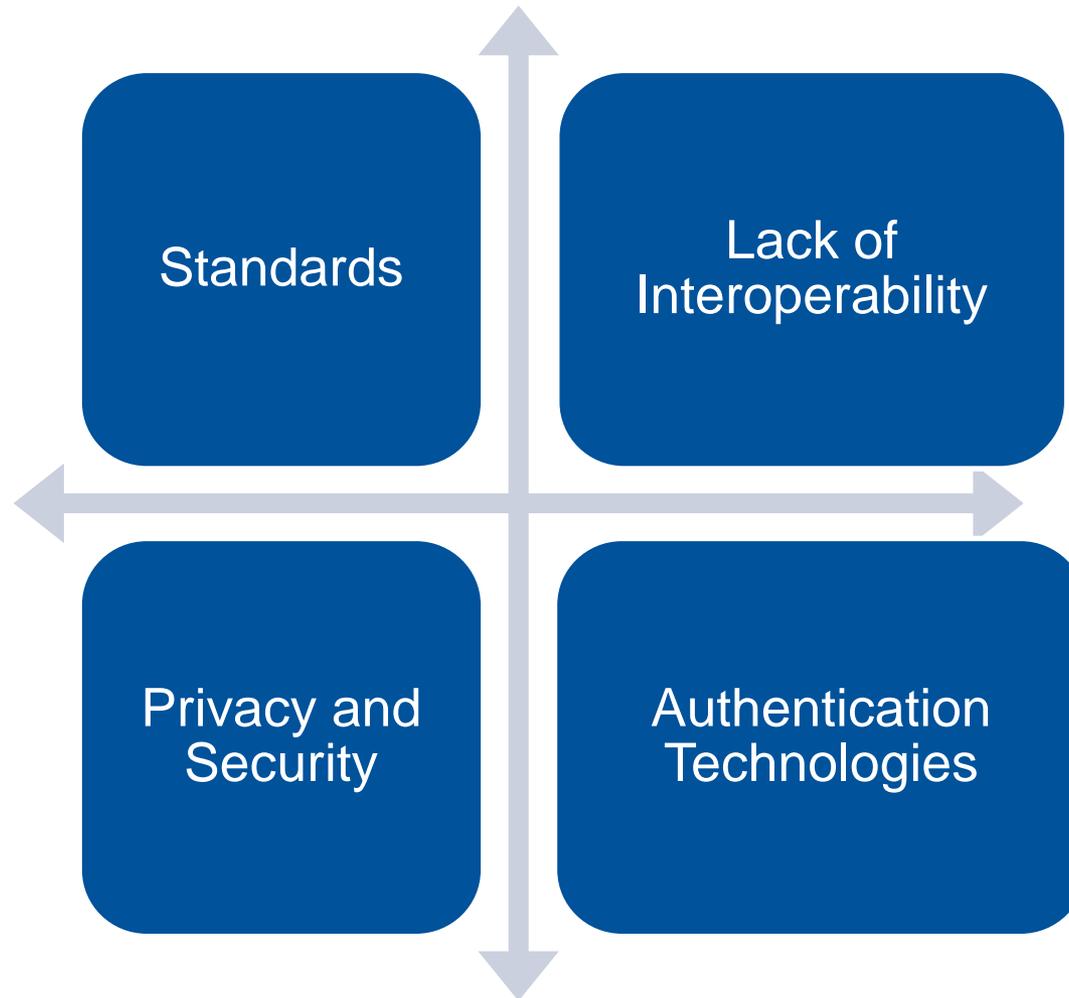
# NSTIC: Two Pillars

---

Private Sector	Government Seed or Cede Landscape
Private Sector Focused	Facilitate and Develop Standards
Innovate for Security and Convenience	Policy Enactments (Legal Frameworks)
Enable Choice for Citizens	Pilot Selection and Funding
New Business Models	Early Adopter

# NSTIC: Overcome the Barriers

---



# NSTIC: Examples

---

- **Creating:** Develop and demonstrate a framework of policies, rules of behavior, and agreements among identity ecosystem stakeholders that can be applied across multiple trust frameworks and providers.
- **Serving:** Interoperability across multiple solution stacks (i.e., smart cards, one-time passwords, other technologies) in an identity ecosystem.



# NSTIC Today and Tomorrow

---

- Federation pervades the expanded identity universe to extend trust.
- Access control can (and should) be more risk-based.
- User provisioning requires an enhanced fulfillment layer.
- Directory services are heavily leveraged to create identity data services — the underpinning of the API economy.

# NSTIC: Lessons Learned

---

- Trust frameworks are driven by communities of interest (COI) who seek market operational efficiencies through business, legal, technical and policy interoperability.
- Federated credentials requires policy changes to enable significant security, user experience (SSO and account creation), and business benefits.
- Current IAM business practices do not always conform to NSTIC and need to be managed in terms of privacy and security enhancements and adoption of risk mitigation strategies.
- UX and ease of use required for adoption.
- Levels of assurance must become more consistent.
- Recombining IAM services using federation as a fulfillment mechanism.
- Applications should be created federation ready.
- Validates client identities across channels.
- Revenue streams must be commercially grounded.

# Recommendations — Next Steps

---

- Next Monday (Organization-centric IAM):
  - For the highest leadership buy-in: Build the business case on enabling the mission of the organization — first, security and privacy — second and IT operational efficiency — third.
  - Use Gartner Hype Cycle to guide technology selection and the Magic Quadrant to guide vendor selection and do not forget OSS.
- Over the Next Year (Federated IAM):
  - The only way forward is spelled standards — open or de facto.
  - Determine level of assurance lower the better.
  - Find your community of trust and join the federation and learn by doing.
- Over the Next Three Years (User-centric IAM):
  - Understand the risk level associated with each claim and its certification.
  - Build your services and data interoperability strategy around that and make sure you have a good migration (exit) strategy for your claims data.

# Action Plan for CIOs

---

## Monday Morning:

- *Determine* how National Strategy for Trusted Identities in Cyberspace will impact your organization or business.
- *Examine* why organizations like yours participate in NSTIC pilot programs.

## Next 90 Days:

- *Determine* how your organization can be enabled through external identity, attribute exchanges and stronger user privacy.
- *Embrace* federation.

## Next 12 Months:

- *Incorporate* risk and security and privacy into IAM deployments.
- *Push* for standards adoption.

# Different Approaches Worldwide

Nation	Business Value System	System Interoperability	UX	Challenges
Canada SecureKey Concierge	Federated identity implementation (online ID or smart card)	Federated ID exchange network (identity broker service)	PC-based, USB card reader portal and mobile accessible	Adoption, certification and compliance
Japan au ID Mobile ID	Federated identity service for online ID to for third-party apps, services and websites	Identity broker service using federated Web protocols (OAuth and OpenID Connect)	Mobile and PC-based	Interoperability frameworks
United Kingdom's Identity Assurance Programme (IDAP)	Piloting compliance for commercial entities issuing and authenticating online IDs	Federated identity services via SAML 2.0 Web profiles and and federated Web protocols (OAuth and OpenID Connect)	Mobile and PC-based	Identity verification, level of access
United States The National Strategy for Trusted Identities in Cyberspace (NSTIC)	Piloting: Federal Identity, Credential, and Access Management (FICAM), Federal Cloud Credential Exchange (FCCX)	Federated identity ecosystem using (OAuth and OpenID Connect) to enable higher levels of assurance	Mobile and PC-based	Liability, privacy, revenue models

# Recommended Gartner Research

---

- [Tutorial: Successful Approaches to Citizen Electronic Identification Initiatives in Government](#)  
Jeff Vining (G00258935)
- [Hype Cycle for Identity and Access Management Technologies, 2014](#)  
Gregg Kriezman (G00263810)
- [Are Mobile Biometrics Ready for the Enterprise?](#)  
Anne Elizabeth Robbins and Trent Henry (G00259859)
- [Leveraging Social and Third-party Identity for Consumers and Other Users \(BYOI\)](#)  
Mary Ruddy (G00263829)