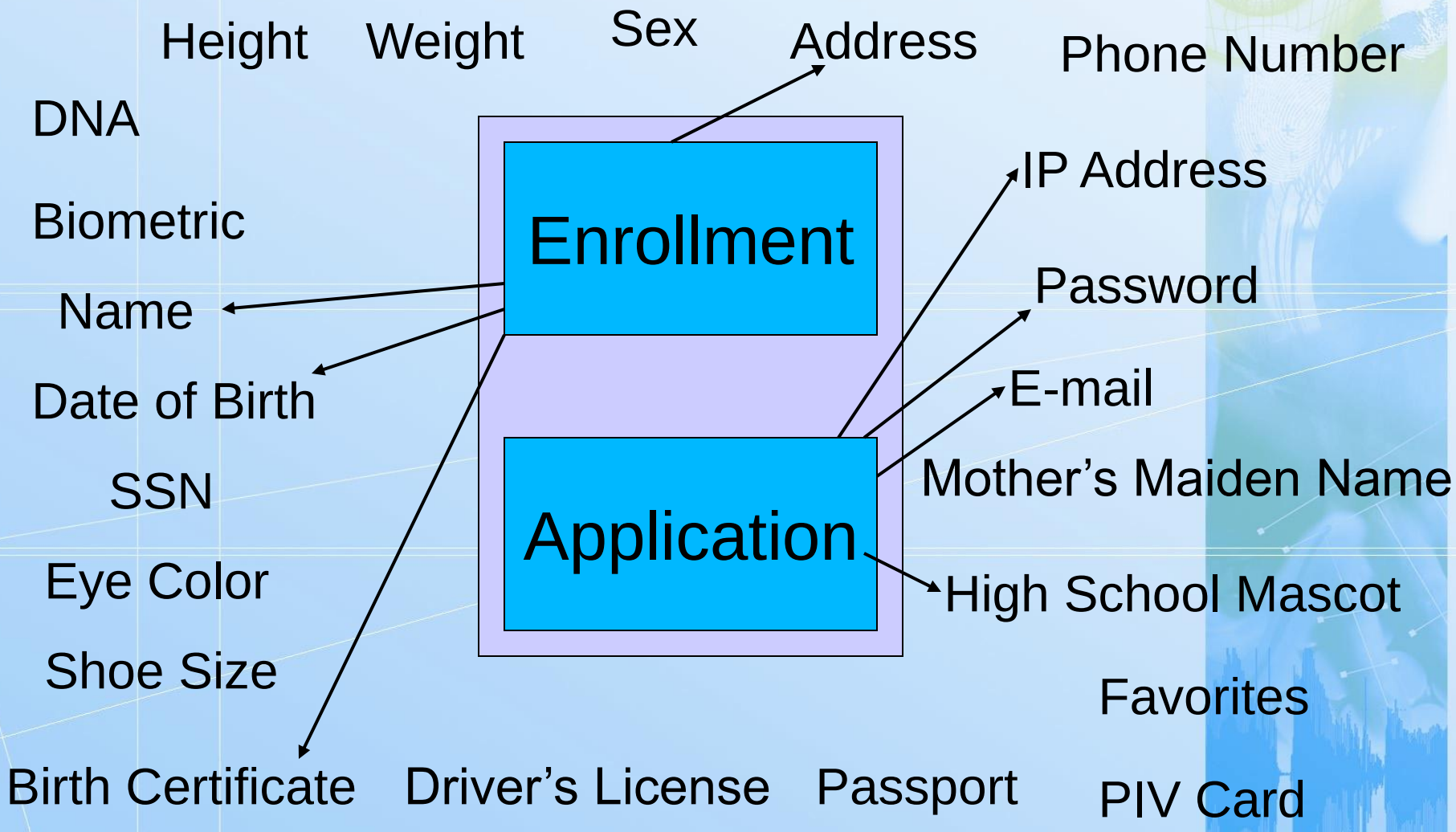
Developing a Federal Vision for Identity Management

Duane Blackburn
Office of Science and Technology Policy
Executive Office of the President

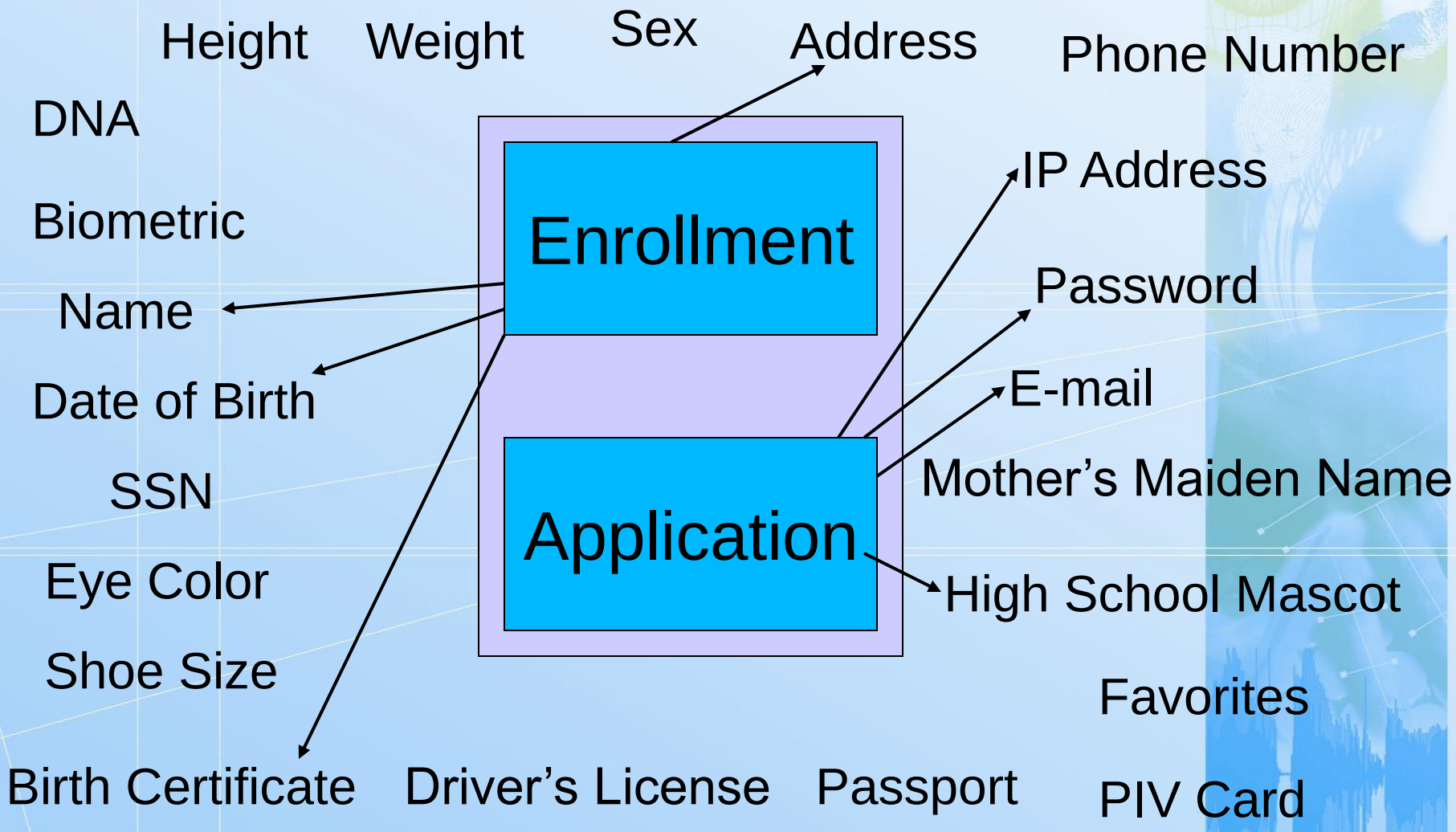
January 16, 2009

Building an IdM System

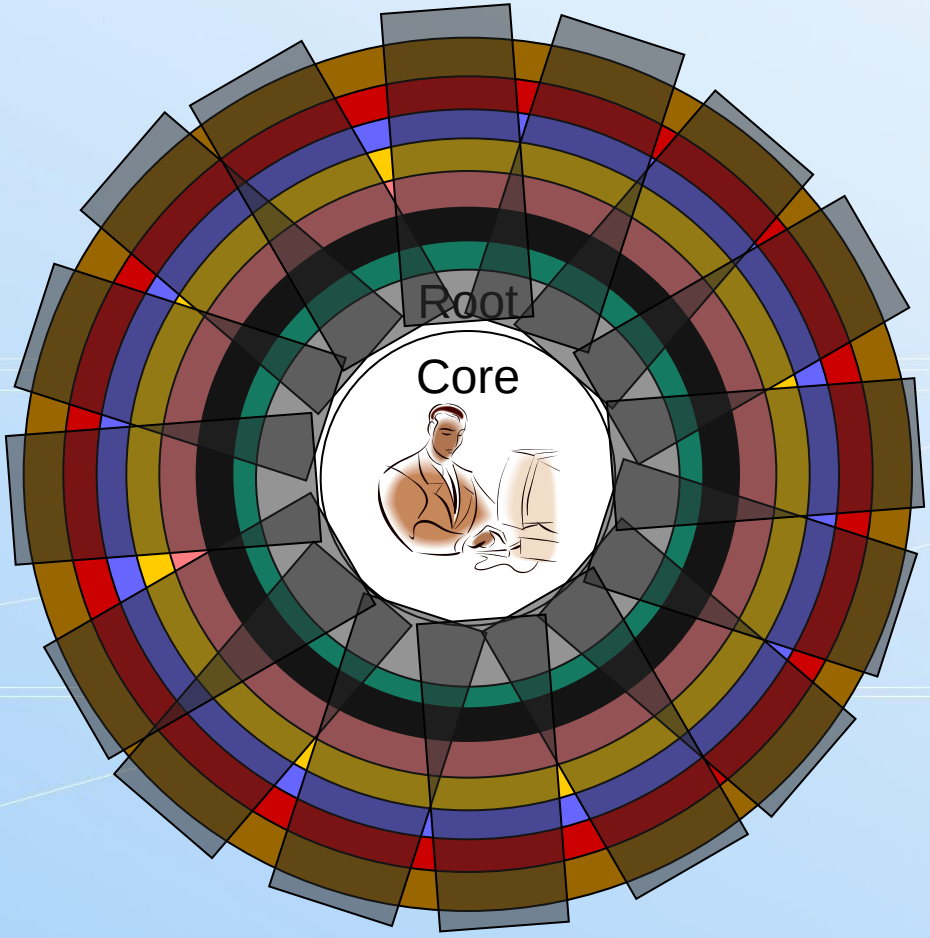



Height
Weight
Sex
Address
Phone Number
DNA
IP Address
Biometric
Password
Name
E-mail
Date of Birth
Mother's Maiden Name
SSN
Eye Color
High School Mascot
Shoe Size
Favorites
Birth Certificate
Driver's License
Passport
PIV Card

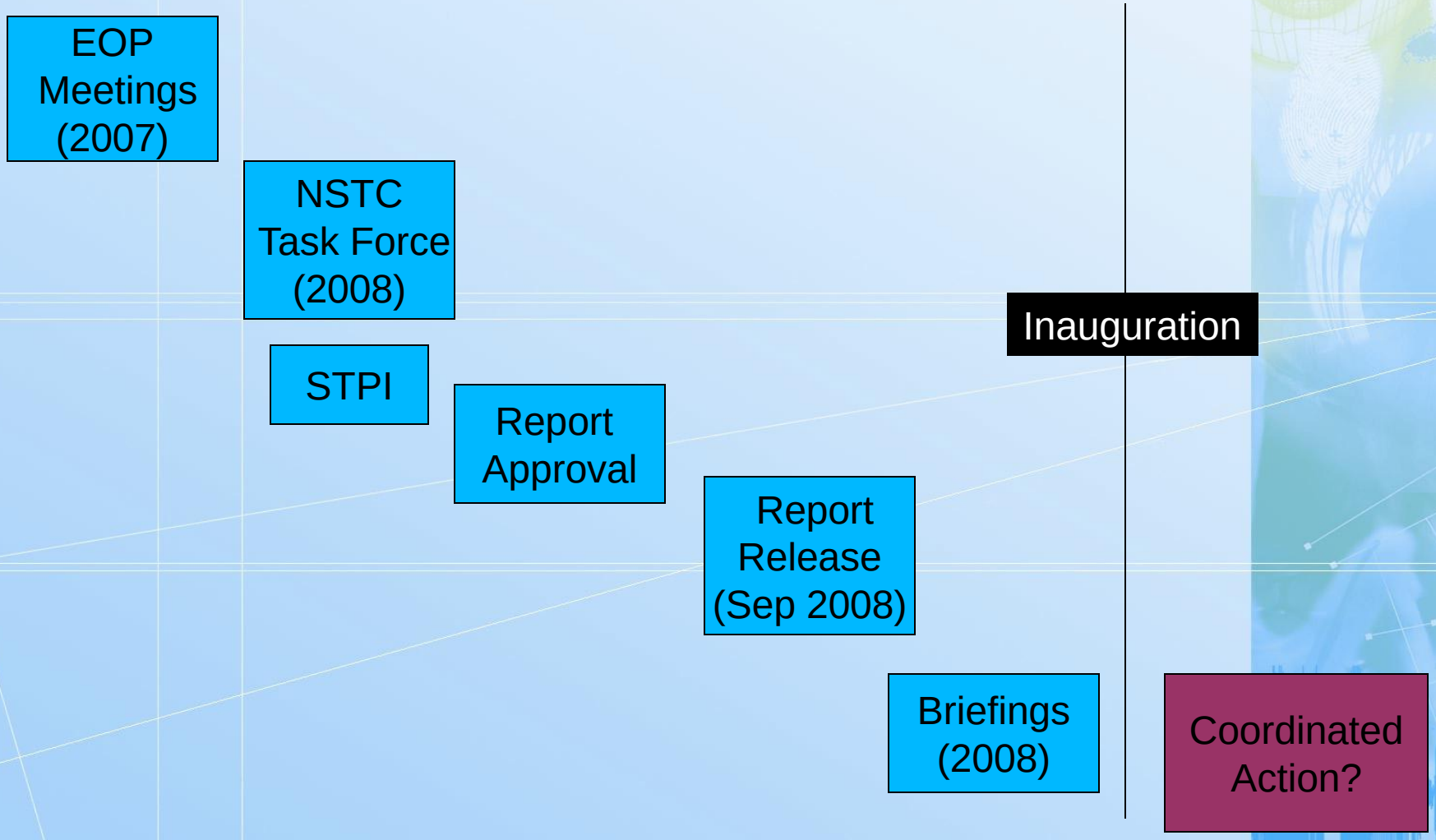
Building an IdM System



Identity Concentricity



Federal IdM Coordination Timeline



Task Force Composition

- Six month effort (January 1 – July 2, 2008)
- Co-chairs
  - Duane Blackburn (OSTP)
  - Judy Spencer (GSA)
  - Jim Dray (NIST)
- Working groups
  - Drafting team
  - Data Collection and Analysis
  - Digital Identity
  - Grid
  - Privacy and Legal
- Participating agencies included DHS, DOD, DOS, DOJ, HHS, SSA, FTC, DOC, GSA, EOP, NSF, ODNI, NASA, FAA, VA, OMB

Task Force Charge

- Provide an assessment of the current state of IdM in the US Government;
- Develop a vision for how IdM should operate in the future;
- Develop first-step recommendations on how to advance towards this vision.

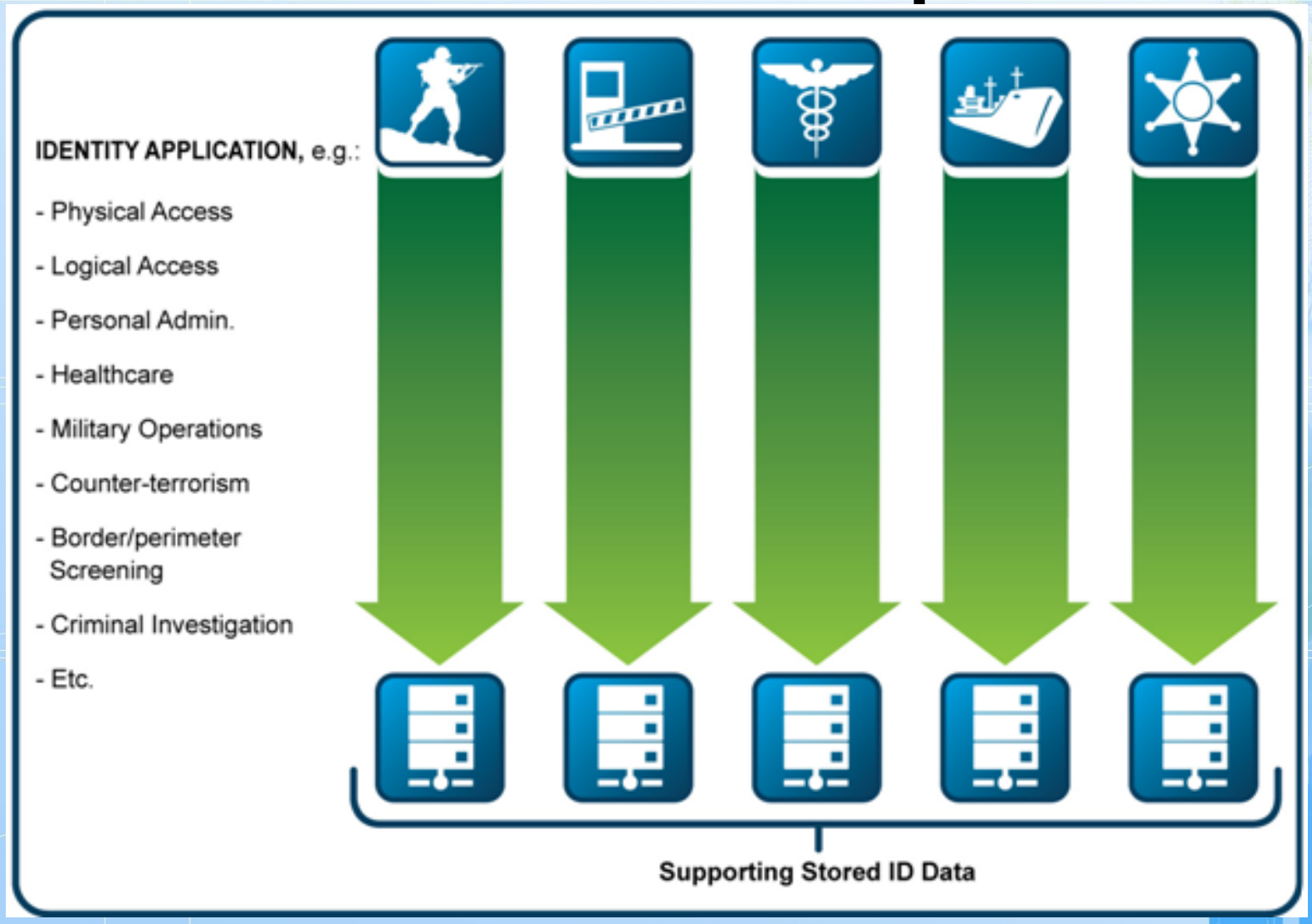
CIO Council Data Call

- First-order understanding of the IdM landscape
- Final Report Appendix G
- 18 responses covering 191 agencies/bureaus, 3400 individual systems
- The most common forms of information being collected for IdM are login alias, PIN/password, legal name, date of birth and social security number
- Few systems (~15%) or programs collect or use biometric-related data (e.g., fingerprints, iris or facial imaging) or use security questions or tokens

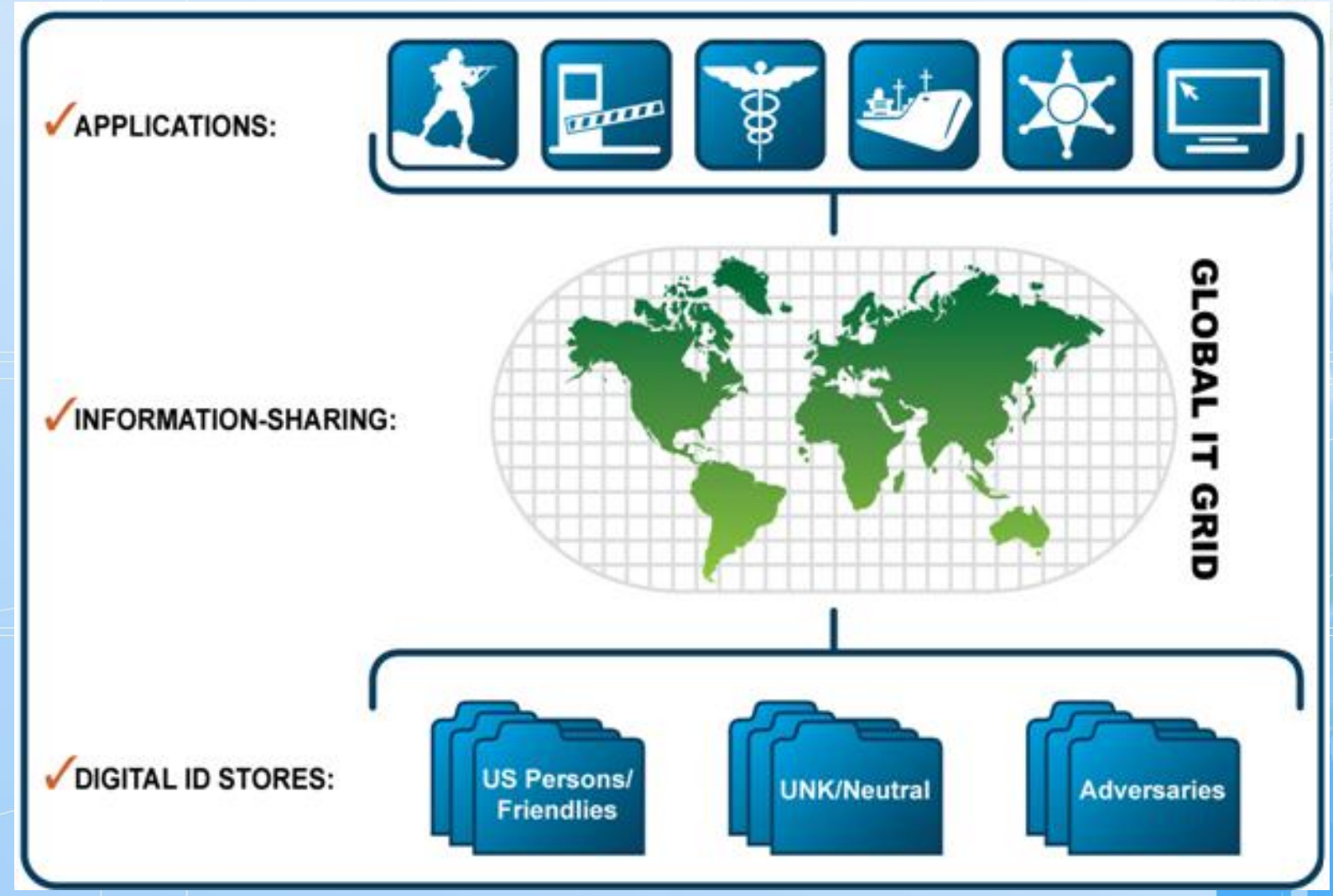
Key Findings of the NSTC IdM TF Report

- IdM is comprised of three elements: ID applications; Global telecommunications grid; Digital ID repositories of all kinds
- Within these, the latter two comprise the "IT Utility"
- Two gross processes of Screening and Access Controls coexist within the USG.
- Public messaging and social acceptance have sometimes been seen as sidebar issues in the USG's approach to IdM, with resultant negative consequences.
- PII may be segregated between application-specific data held inside applications, and that used to establish authentication of basic digital ID's.
- USG missions include extensive engagement with other jurisdictions of government, international partners, and the public. This underlines not only the criticality of treatment of PII, but also the need for federal processes to be attuned to commercial and emergent international IdM approaches, standards and systems.

Current Landscape

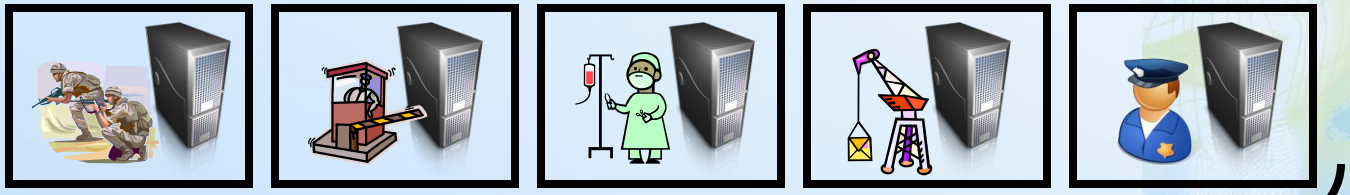


Future State Vision



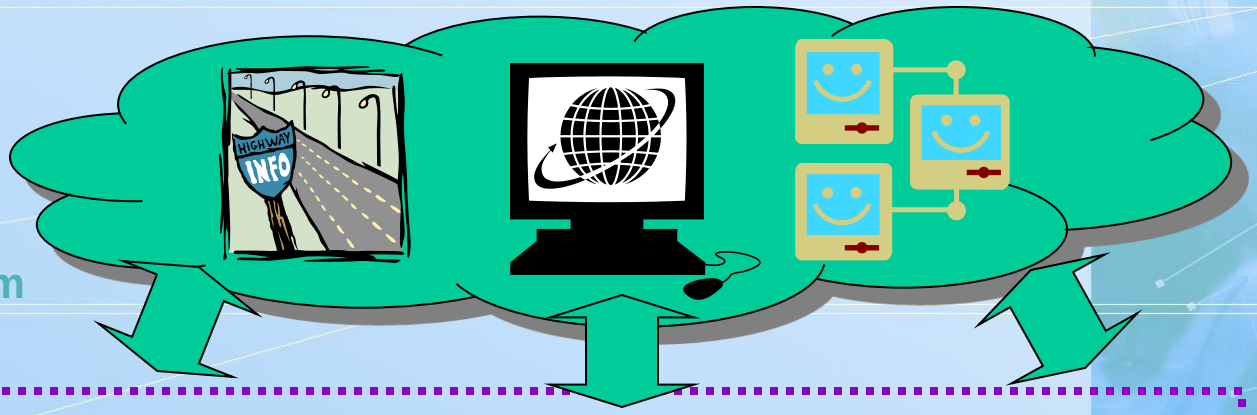
Objective IdM Architectural Model

ID-specific "Privileges" (Applications of ID in specific context), with *data unique to each*



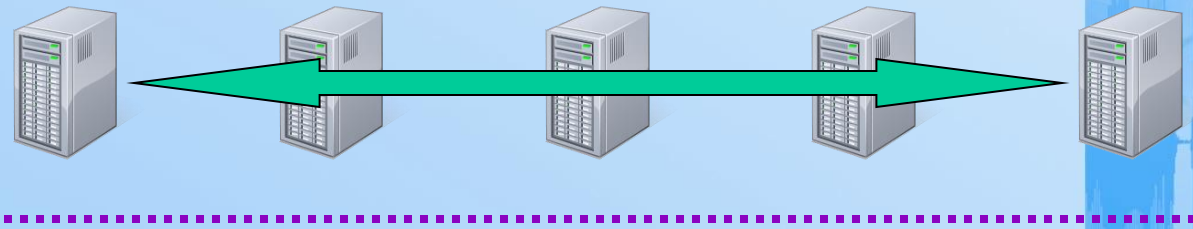
Application/user Interface

Identity Management "Utility"



Enterprise IT System

'Network of Networks' *Digital ID Data* Federation



IdM Refocus

CHARACTERISTIC:	TODAY	Future
Focus:	Data sets	Applications
Challenges:	Standards; Social acceptance	Scalability; Business models
Controlling Equity:	Federal IT community	Balanced equities - End users - Application sponsors/managers - Digital ID managers - Global grid/IT managers
Cultural Character:	Service-provider push	User-demand pull
"Appearance":	German watchmaker's shop	Utility (elex pwr analogy)

Key recommendations

- **12 prioritized R&D recommendations**
  - Rationale: Tech base supporting IdM decomposed, with investments (hopefully) leading to process improvements proposed in each major area
- **Complete the basic as-built research, in full detail**
  - Applications, processes, etc
- **Conduct gap analysis**, and from that, detailed **strategy**
- **Architectural framework…**
  - Singular, comprehensive, interoperable
  - Standards-based
  - Privacy-centric
  - Security-conscious
- **Advance the Global Grid agenda**
  - Next-generation network(s)
  - Engage internationally
- **Governance**

TF Report Available online

- www.ostp.gov/nstc
- www.biometrics.gov
- www.idmanagement.gov

You are not alone…

- President's Identity Theft Task Force
- NSTC, IdM Task Force
- CIO Council, Information Security and IdM Committee
- Information Sharing Environment, IdAM Framework
- National Security Telecommunications Advisory Committee, IdM Task Force
- HSPD 6, 11, 12
- NSPD-59
- Cybersecurity Initiative
- Organisation for Economic Co-operation and Development (OECD)
- International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)
- Naval Post Graduate School, IdM degree program
- Many others…

Duane's Key Take-Home Points

- Identity and appropriateness of IdM varies amongst individuals
- Numerous IdM activities in the USG
  - Which represent a fraction of IdM activities in the US/World
  - Activities in one impact others
- If we continue to build our systems as if it was to be the only system in existence, we are building our system to fail
- If we continue to build our system-of-systems as if our sector was the only one with identity issues, we are building our system-of-systems to fail
- How are we going to move forward?