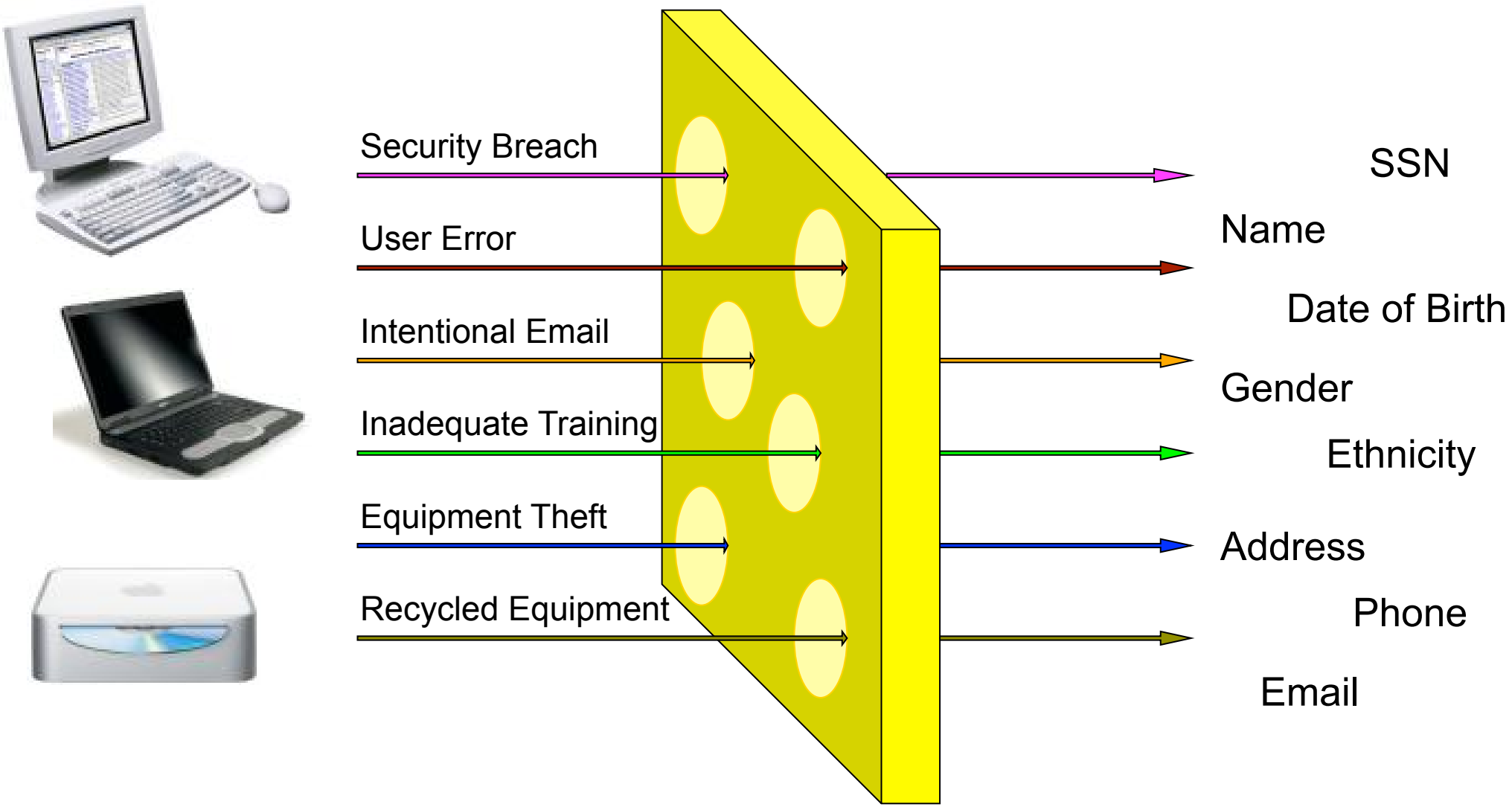
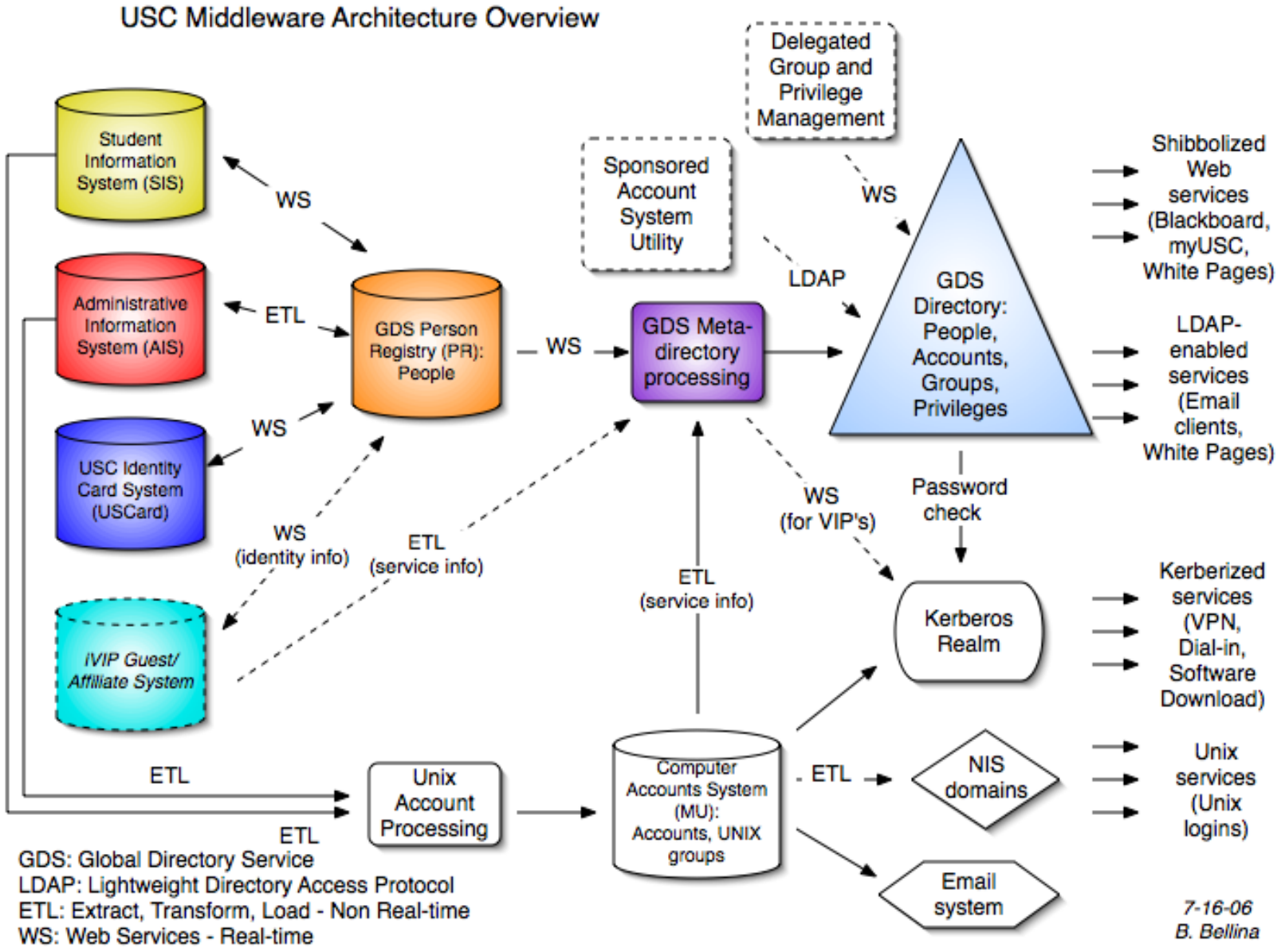
USC
INFORMATION
TECHNOLOGY
SERVICES

Applying Data Governance in Identity Management: To Serve and Protect

Brendan Bellina
Identity Services Architect
Information Technology Services
University of Southern California
bbellina@usc.edu

Distributed Data = Leaks




USC Middleware Architecture Overview
Student Information System (SIS)
Administrative Information System (AIS)
USC Identity Card System (USCard)
iVIP Guest/ Affiliate System
GDS Person Registry (PR): People
Unix Account Processing
Sponsored Account System Utility
Delegated Group and Privilege Management
GDS Meta-directory processing
GDS Directory: People, Accounts, Groups, Privileges
Computer Accounts System (MU): Accounts, UNIX groups
Kerberos Realm
NIS domains
Email system
Shibbolized Web services (Blackboard, myUSC, White Pages)
LDAP-enabled services (Email clients, White Pages)
Kerberized services (VPN, Dial-in, Software Download)
Unix services (Unix logins)
WS
ETL
LDAP
Password check
WS (identity info)
ETL (service info)
WS (for VIP's)
ETL (service info)
GDS: Global Directory Service
LDAP: Lightweight Directory Access Protocol
ETL: Extract, Transform, Load - Non Real-time
WS: Web Services - Real-time
7-16-06
B. Bellina

Development of the Person Registry (PR)

- Establishes authoritative Person ID - USCID
- Real-time communication with primary SORs (SIS, AIS, iVIP, USCard)
- Stores/matches identifying data - name, Date of Birth, Social Security Number
- Required agreements on:
  - Common data definitions (DOB and SSN),
  - Data ownership hierarchy for updates
  - Policies for merging identities and USCIDs

Development of the Global Directory Service (GDS)

- GDS "cloud" includes PR, MU, the interfaces to them: GDS LDAP and Shibboleth; and metadirectory processes
- Nightly updates to active person, account, and groups information based on inputs from MU, the PR, and group exceptions
- Provides authentication, authorization, attributes, and group services through LDAP and Shibboleth
- Required agreements on:
  - Standard schema definitions (eduPerson, eduCourse),
  - Access controls for anonymous and authenticated queries
  - Request process for data access and group definitions
  - Policies on addition of new data elements and types

- **Data Governance brings together cross-functional teams** to make interdependent rules or to resolve issues or to provide services to data stakeholders. These cross-functional teams - Data Stewards and/or Data Governors - generally come **from the Business side of operations. They set policy that IT and Data groups will follow** as they establish their architectures, implement their own best practices, and address requirements. Data Governance can be considered the overall process of making this work.

- http://www.datagovernance.com/adg_data_governance_governance_and_stewardship.html

When to use formal Data Governance

- When one of four situations occur:
  - **The organization gets so large** that traditional management isn't able to address data-related cross-functional activities.
  - **The organization's data systems get so complicated** that traditional management isn't able to address data-related cross-functional activities.
  - The organization's Data Architects, SOA teams, or other horizontally-focused groups **need** the support of a cross-functional program that takes **an enterprise** (rather than siloed) **view of data** concerns and choices.
  - **Regulation**, compliance, or contractual requirements call for formal Data Governance.
  - http://www.datagovernance.com/adg_data_governance_basics.html

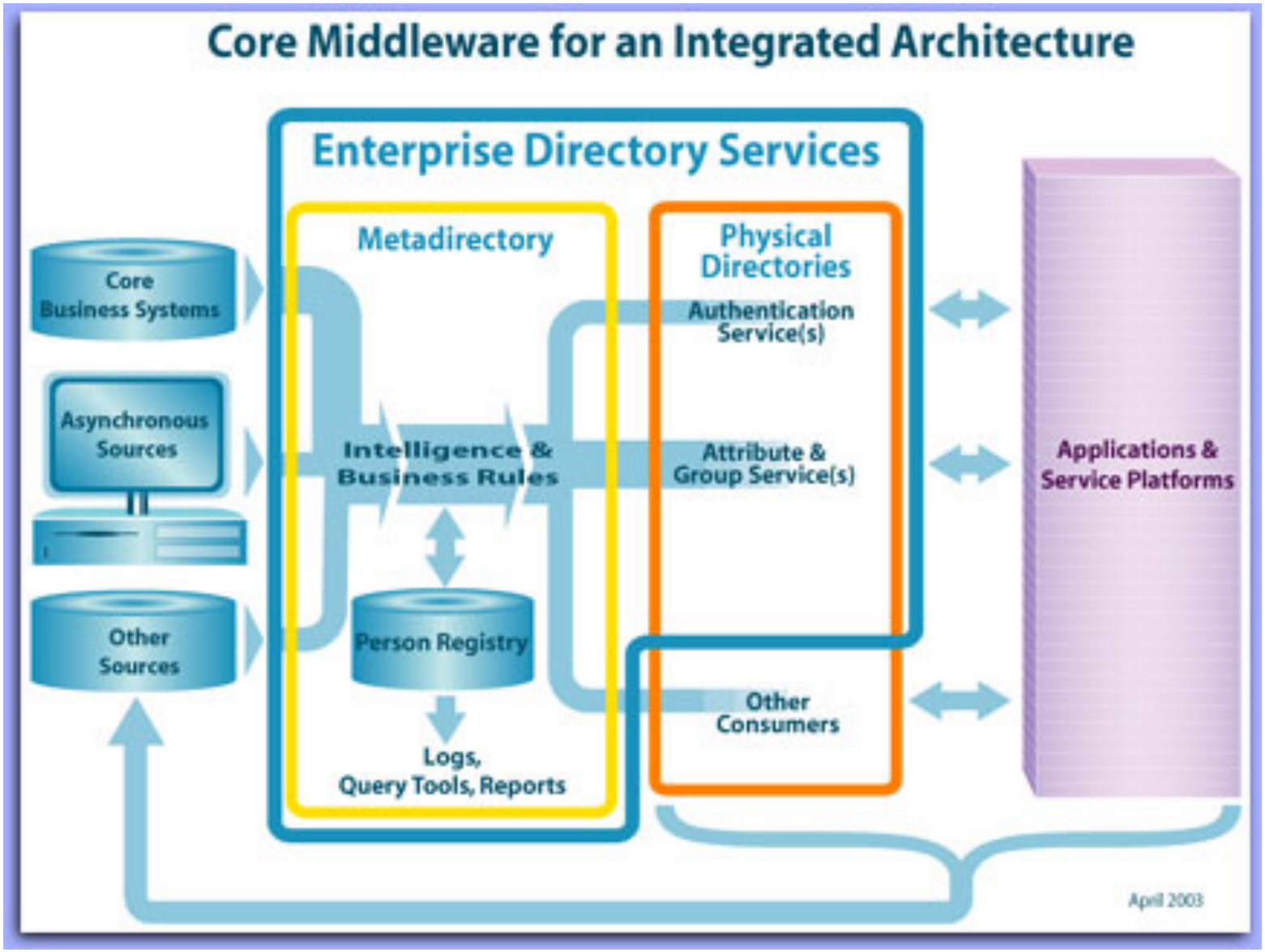
Data Governance Principles

- Eight Principles:
  - Integrity
    - All data requests are reviewed in committee, including central IT requests
    - No rubber-stamping. No railroading. No exceptions.
  - Transparency
    - Committee meetings are open and held during lunch hours.
    - Policies are posted on GDS website
  - Auditability
    - All Data Requests are retained and tracked in the USC Wiki
  - Accountability
    - Data Access is granted only following approval. No technical overrides.
- http://www.datagovernance.com/adg_data_governance_goals.html

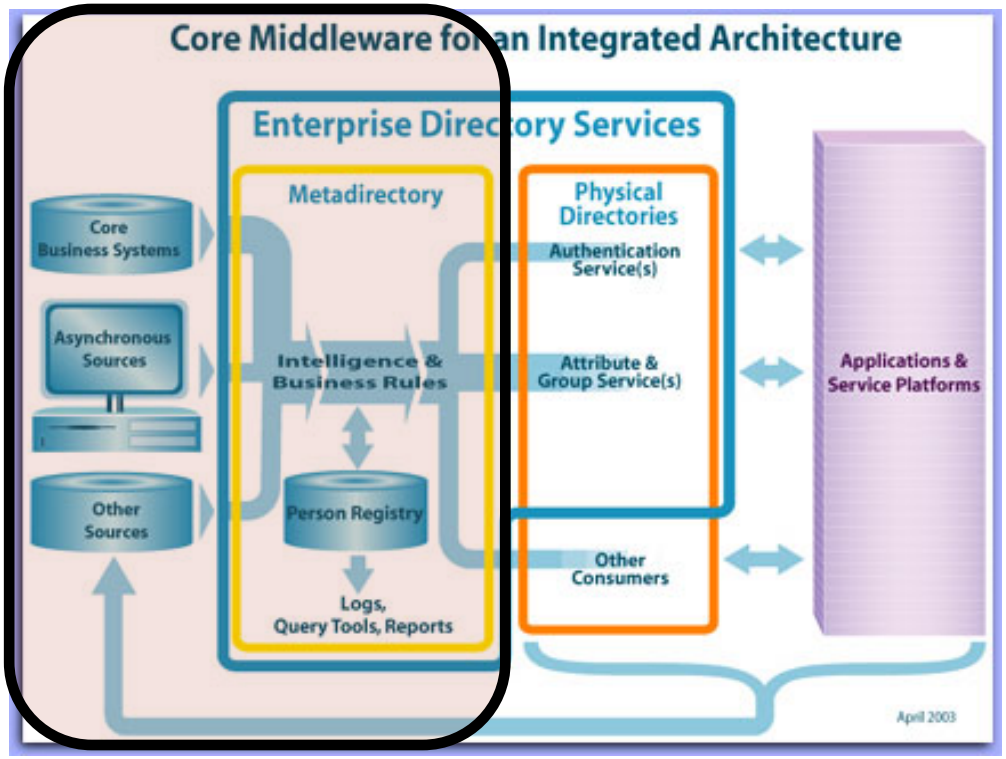
- Stewardship
  - Data Stewards must review and approve all data requests.
  - Department IT leaders are engaged in the review process.
- Checks-and-Balances
  - ITS Architect attends all meetings but does not vote.
  - All requests go through a meeting with ITS prior to committee to ensure all appropriate questions are considered.
  - ITS makes no production changes for data release without committee approval.
- Standardization
  - Establish sub-committees and spin-off efforts to determine standardization on role definitions and data usage.
  - USC is an active participant in relevant collaborative standards development (MACE-Dir, Internet2, EDUCAUSE, InCommon working groups).
- Change Management
  - Requests are maintained in the USC Wiki
  - Access control changes are maintained as prior versions for historical review

IAM Data Governance Committees

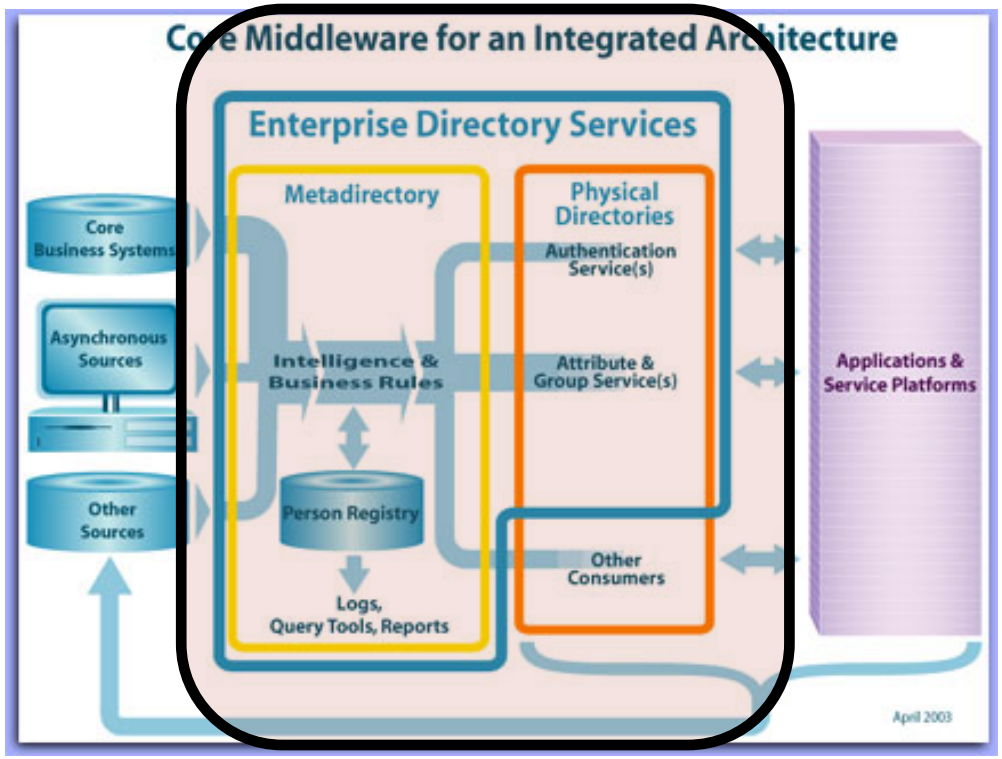
- All committees are chaired by the Director of the Office of Organization Improvement Services, Margaret Harrington.
- **Directory Steering Committee** - management committee meets every 3 weeks
  - focuses on policy regarding data acquisition and release, integration, and communication
  - attendees include senior management representatives from academic schools, administrative departments, IT Security Office, General Counsel
- **GDS Executive Committee** - management committee every other week
  - focuses on technical and staffing issues affecting direction and prioritizations
  - attendees include management representatives from SOR's and GDS team
- **Data Team** - technical committee meets every 3 weeks
  - focuses on operational issues affecting SOR's and PR/GDS
  - attendees include representatives from SOR's and GDS team


Core Middleware for an Integrated Architecture
Enterprise Directory Services
Metadirectory
Physical Directories
Core Business Systems
Asynchronous Sources
Other Sources
Intelligence & Business Rules
Person Registry
Logs, Query Tools, Reports
Authentication Service(s)
Attribute & Group Service(s)
Other Consumers
Applications & Service Platforms
April 2003

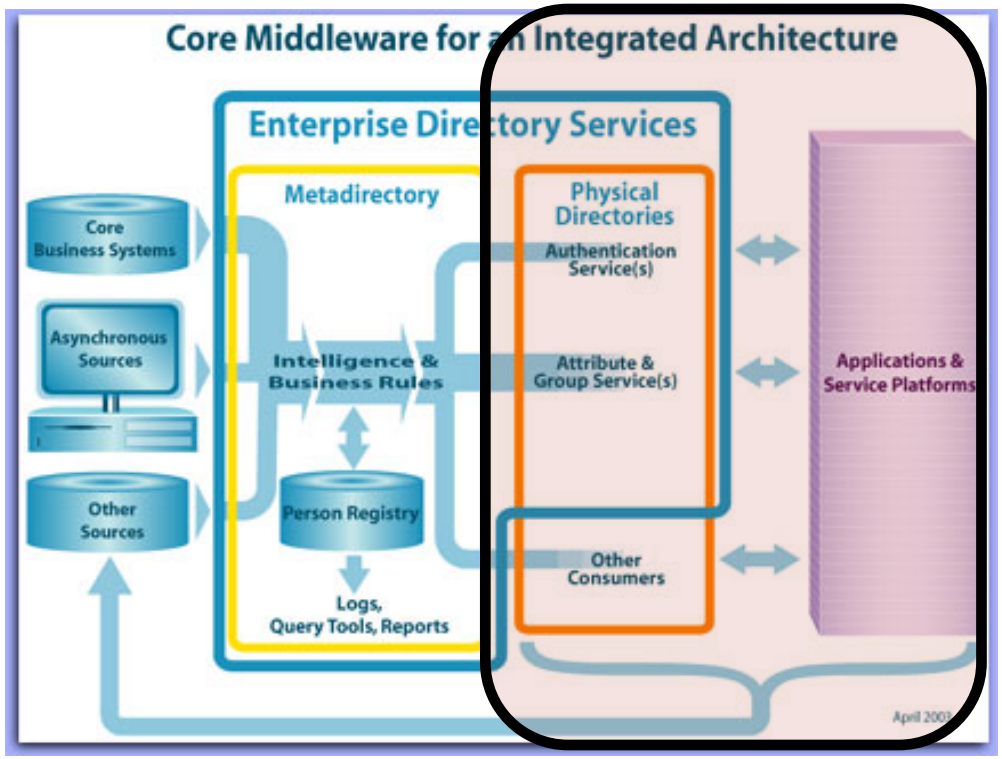
Data Team


Core Middleware for an Integrated Architecture
Enterprise Directory Services
Metadirectory
Physical Directories
Core Business Systems
Asynchronous Sources
Other Sources
Intelligence & Business Rules
Person Registry
Logs, Query Tools, Reports
Authentication Service(s)
Attribute & Group Service(s)
Other Consumers
Applications & Service Platforms
April 2003

GDS Executive Committee



Directory Services Steering Committee



Role of Central IT in Data Governance

- Central IT is NOT a data steward
- Central IT is a subject matter expert regarding technology
- Central IT is implementer, NOT policy maker
- Central IT provides an enterprise view, providing a counter-balance to department-centric development
- Central IT acts as a representative of the institution in the development of external standards

Attribute Access Request Process

- Documented at GDS website
- Chaired by Director of the Office of Organizational Improvement
- Required for all data requests to GDS content
- Meeting with ITS and application sponsor occurs prior to Directory Steering Committee
- Directory Steering Committee reviews all new requests
- Data Stewards must approve requests
- Requests must be reauthorized every 2 years

Authorization Model

- Service Provider must explicitly define user population
  - based on attributes in the GDS provided by the SOR's, or
  - as a discretionary (exception) group recorded in the GDS
- GDS Authorization Group is used to record the application user population and assign an entitlement for the service
- Shibboleth (or LDAP) releases attributes to the Service Provider only for users with the entitlement value for the service
- *Authorization to use a service is determined at the Identity Provider based on GDS attributes BEFORE any attributes about the user are released to the service.*

Challenges

- Maintaining consistent engagement of departmental leaders
- Perception of governance process being a barrier to rapid deployment of services
- Services without Sponsors
- Lack of Knowledge Leading to Missteps and Resistance
- Persisting Contrary IT Practices
  - Departmental portals and proxies grouping users and data
  - Lack of data requirements for projects
  - Allowing major projects to bypass governance and review
  - Fabricated accounts in production to facilitate support
  - Shadow and test systems providing access to production data
  - Administrators taking liberty with data access when pressed

Links

- USC GDS website: http://www.usc.edu/gds
- Additional Presentations: http://its.usc.edu/~bbellina
- Contact the author via email: bbellina@usc.edu