

Interagency Advisory Board

Meeting Agenda, March 5, 2009

1. **Opening Remarks (Tim Baldrige, NASA)**
2. **Federal Identity, Credential, and Access Management (ICAM) – The Future of the Government's IDM Strategy (Judy Spencer, GSA)**
3. **Co-Development of PKI/BLADE and PIV: Requirements and Roadmaps (Jarrod Frahm, DOS and Bill Macgregor, NIST)**
4. **Winter Chill Exercise Debrief (Craig Wilson, FEMA)**
5. **MSO SSP Update (Steve Duncan, GSA)**
6. **PAIIWG Update (Tim Baldrige, NASA)**
7. **Closing Remarks (Tim Baldrige, NASA)**



Identity, Credential and Access Management The Government-wide Initiative

Judith Spencer
Agency Expert - IDM
Office of Governmentwide
Policy
General Services Administration



Consolidation of Identity Management Activities

- NSTC Identity Management Task Force Report
 - Identified need for consolidation/executive level oversight of identity management activities.
- CIO Council established the Information Security and Identity Management Committee (ISIMC)
 - Provide executive level oversight to Cybersecurity and Federal IDM activities
- ISIMC established a new subcommittee on Identity, Credential, and Access Management
 - Encompass E-Authentication, Federal PKI, and HSPD-12 activities

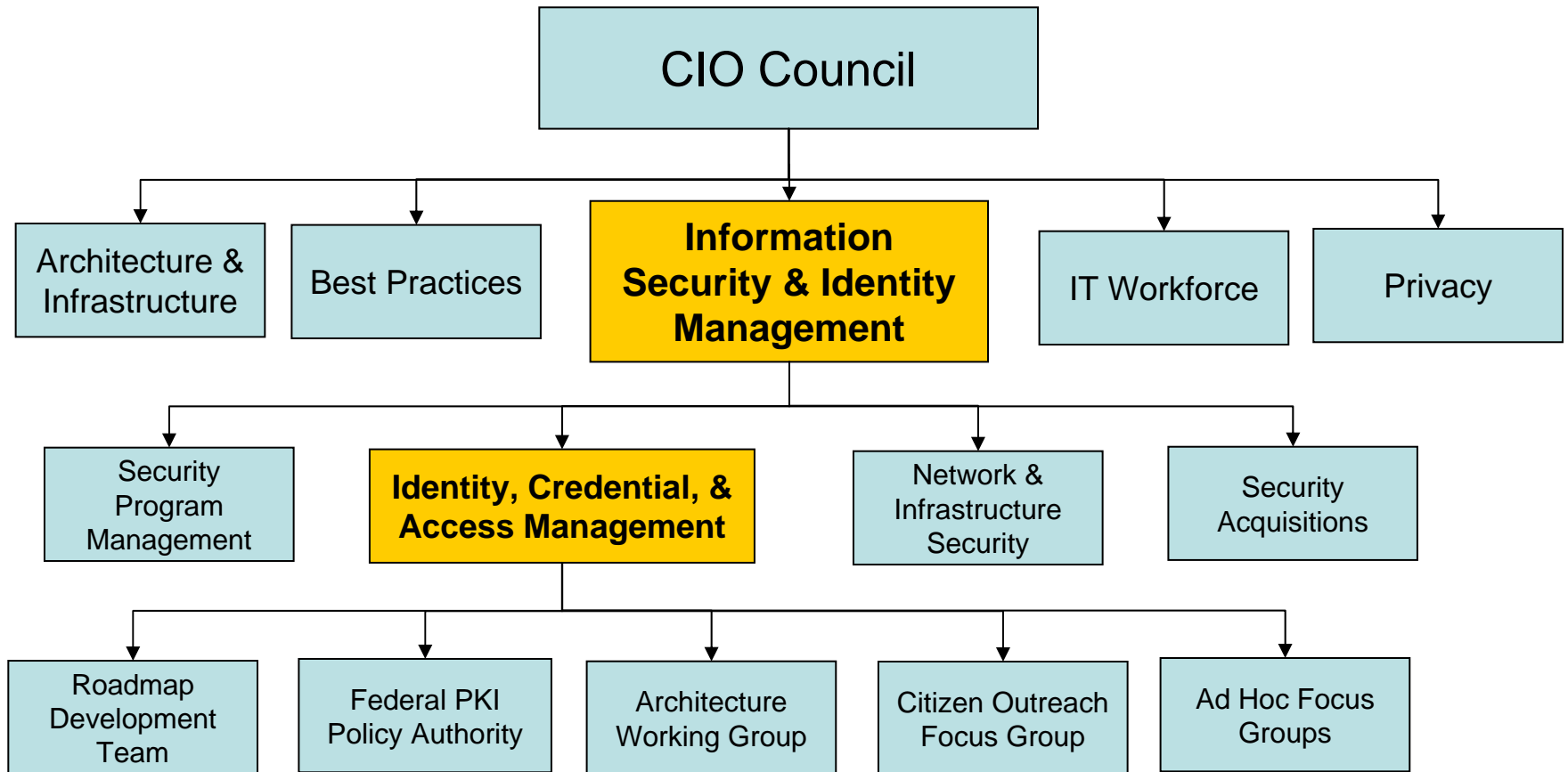


ISIMC

Co-Chairs: Vance Hitch, DOJ & Rob Carey, DON

- Develop strategies to coordinate and facilitate the execution of the *Comprehensive National Cybersecurity Initiative* (CNCI) (National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)).
- Identify and recommend information security and identity management enhancements to policies, processes, and solutions, that address the strategies in (A) above and improve upon identification management solutions.
- Provide oversight of the ISIMC subcommittees, working groups, and task forces. Coordinate with and provide advice to other Federal committees to improve collaboration, identify complimentary activities, and reduce duplication in security and identity management related areas. Review and concur on common security management requirements, performance measures, and Federal Enterprise Architecture (FEA) updates, program management plan, fiscal budget and funding strategy for security management service areas.
- Promote the development and use of standard performance measures for agency information security.
- Share experiences and innovative approaches related to information sharing and information security best practices that span both defensive operational security such as penetration testing regimes, and incident response mitigation, and span security policies compliance, such as FISMA or PMA achievement.
- Identify common Computer Information Security Officer (CISO) and information assurance professional qualifications in coordination with the FCIOC IT Workforce Committee.

New Committee Structure



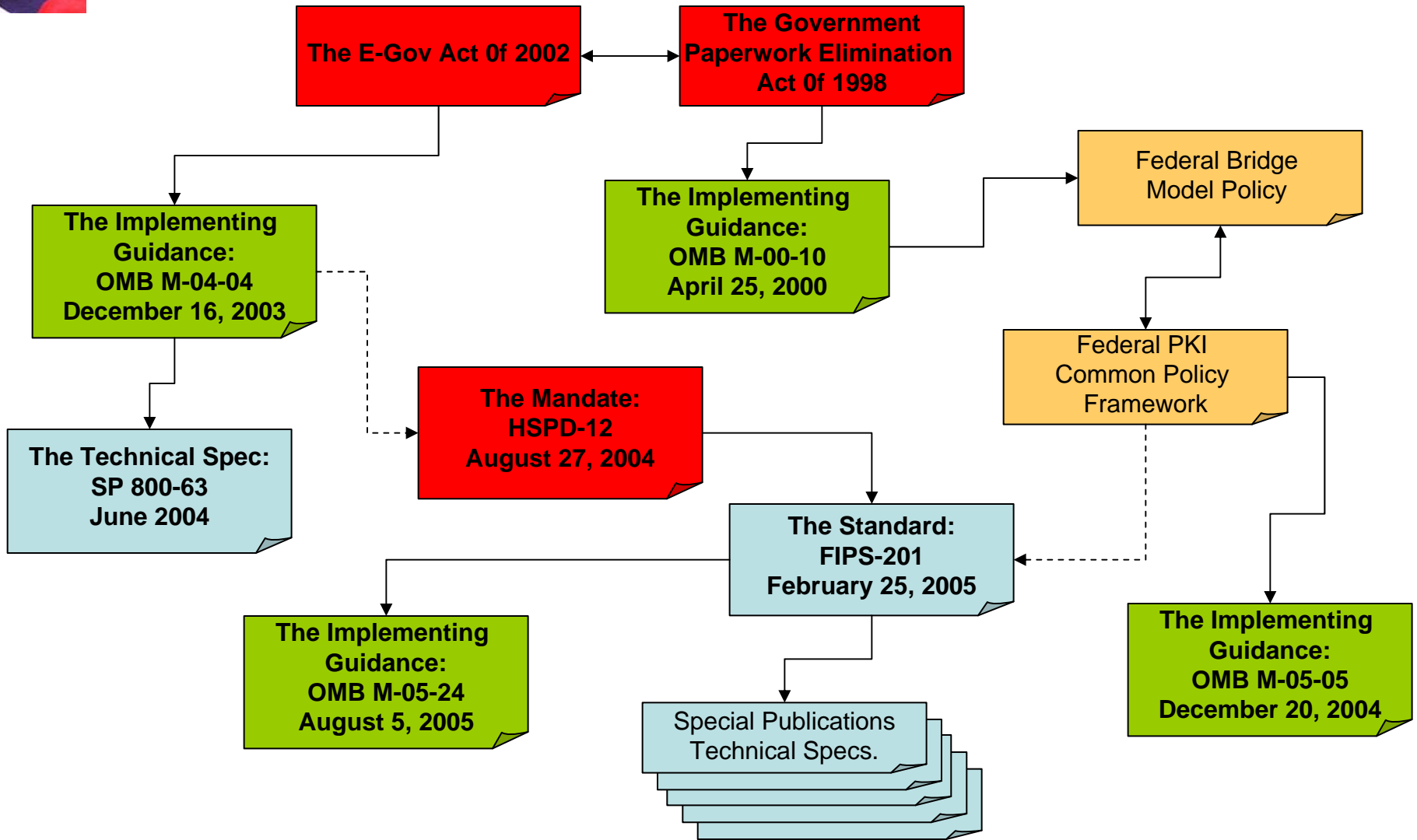


ICAM Mission

- Fostering effective government-wide identity and access management
- Enabling trusted in online transactions through common identity and access management policies and approaches
- Aligning federal agencies around common identity and access management practices
- Reducing the identity and access management burden for individual agencies by fostering common interoperable approaches
- Ensuring alignment across all identity and access management activities that cross individual agency boundaries
- Collaborating with external identity management activities through inter-federation to enhance interoperability

Co-Chairs: Paul Grant, DOD & Judith Spencer, GSA

Enabling Policy and Guidance





4 Sectors for Government Interaction

Government to Citizen

Government to Business

E-Authentication Guidance (M-04-04)

**Government to
Government**

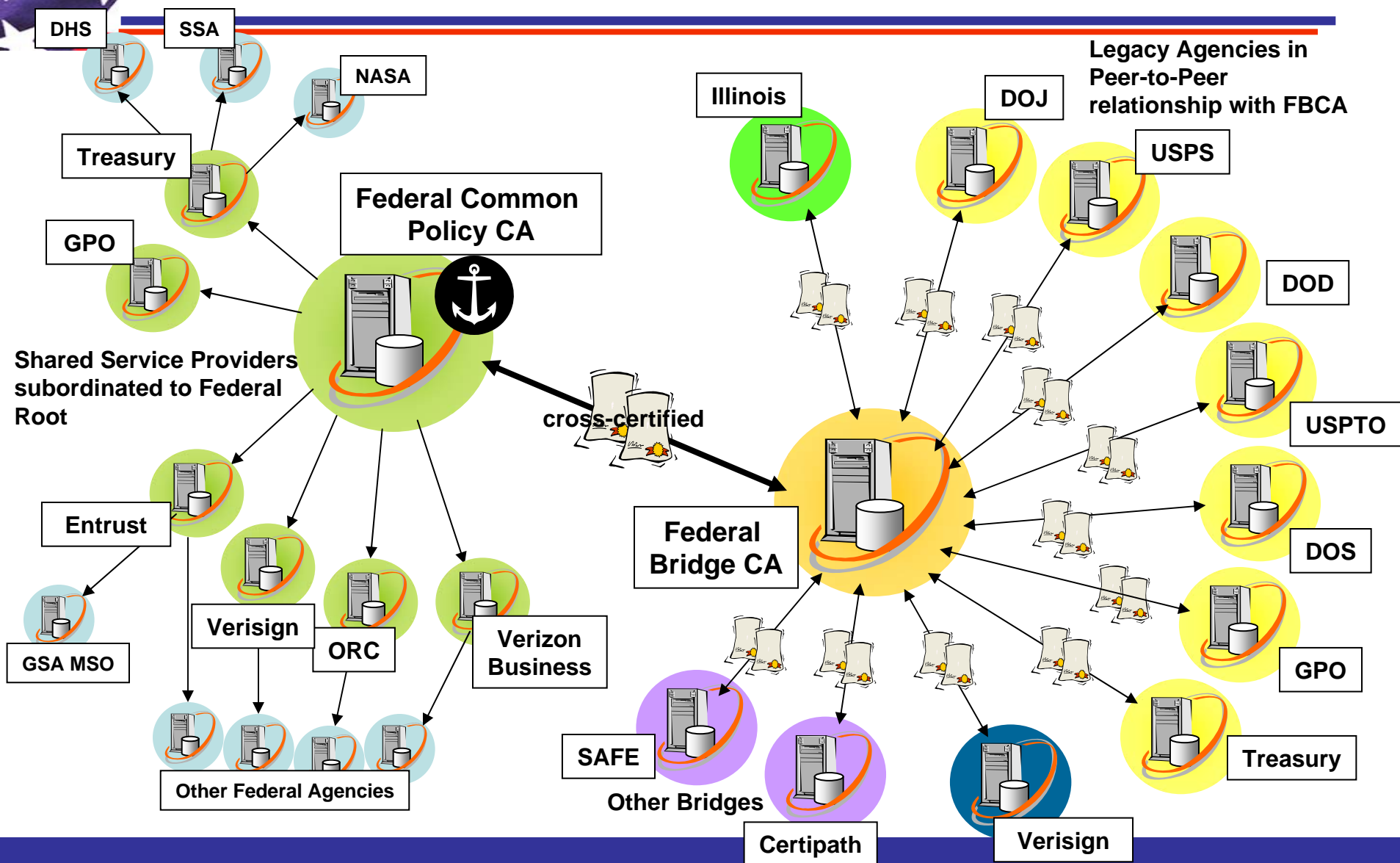
HSPD-12
Internal Effectiveness
and Efficiency



Increasing the Trusted Credential Community

- Back to Basics – M-04-04 and NIST 800-63 are still the foundational policy/technical guidance for identity management.
- Establish unified architecture for Identity Management
- Expanding our use of Assertion-based solutions (Levels 1 & 2)
 - Partnering with Liberty Alliance
 - Stronger industry alignment for trust and technology standards
- Federal Bridge will continue to play a role at Levels 3 & 4
 - External Shared Service Providers
 - Four Bridge Forum (FBCA, Certipath, SAFE-BioPharma, HigherEd)
 - Transglobal Secure Collaboration Program
- Outreach to communities of interest
 - InCommon – Post-secondary education community
 - Explore natural affinities

Federal PKI Trust Framework





Next Steps

- Publish *PIV Interoperability for Non-Federal Issuers* guidance
- Publish *ICAM Roadmap & Implementation Guide*
 - Includes IDM Segment Architecture
- Establish Citizen Outreach Focus Group
- Continue Outreach Activities
 - Liberty Alliance Partnership
 - Transglobal Secure Collaboration Program
 - Educause (post-secondary education)