CSDII
Cross Sector Digital
Identity Initiative

AAMVA – CSDII NSTIC Pilot Trust Framework Gap Analysis

Presentation to the NIST National Program Office

19 March 2013

CSDII
Cross Sector Digital Identity Initiative

Agenda

- **Purpose**
- **Model Trust Frameworks (TFs)**
- **Methods & Assumptions**
- **Analytic Device**
- **Detailed Walk-through**
- **Next Steps**

CSDII
Cross Sector Digital Identity Initiative

Purpose

- Assess model trust frameworks (TFs) on business, legal, technical and "other" (BLT-O) dimensions using analytic device
- Evaluate how selected model TFs aligned with TF requirements for the CSDII Pilot
- Identify elements and sample agreements from model TFs that may be "reused" for the CSDII Pilot TF

CSDII
Cross Sector Digital Identity Initiative

Model TFs

- AAMVA DL/ID Security Framework
- eHealth Exchange DURSA
- InCommon TF
- Kantara Initiative TF
- Open Identity Exchange (OIX)/OITF
- CIVICS/IDCubed.org TF

CSDII
Cross Sector Digital Identity Initiative

Methods & Assumptions

- Built from existing research and COV experience to develop analytic device covering BLT-O dimensions
- Framed analysis on elements and agreements in model TFs that could be directly applied for the CSDII Pilot
- Assumed that the CSDII TF would need to be scalable (horizontally & vertically) and support post-pilot implementation

CSDII
Cross Sector Digital Identity Initiative

Analytic Device

	Trust | Security Frameworks – Key Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Trust | Security Framework Comparison	• Definitions for "Permitted Purpose" • Governing Body & Change Processes • Operating Policies & Procedures • Security, Privacy & Confidentiality-Business: Consent/Auth.) • Suspension & Termination (Voluntary & Involuntary) • Data Elements & Data Classification (Attribute Level/PII) • Expectations of Performance • Use Cases (Exchange & Participant Types)	• Definition/Identification of "Applicable Law" • Legal Agreements (Set) for Exchange Structure (IdPs/RPs/ITSPs) • Security, Privacy & Consent Provisions • Assignment of Liability & Risk for Participants • Representations & Warranties • Grant of Authority • Dispute Resolution • Authorizations for Data Requests by Participant • Open Disclosure & Anti-Circumvention • Confidential Participant Information • Audit, Accountability & Compliance	• Performance & Service Specifications • Security, Privacy & Confidentiality (Technical: Infrastructure/ Architecture) • Breach Notification • System Access (ID/Authentication) • Provisions for Future Use of Data • Duty of Response by Participants (IdPs/RPs/ITSPs) • Onboarding, Testing & Certification Requirements • Handling of Test Data v. Production Data • Compliance with External/SDO Standards	• Openness & Transparency • TF Lifecycle Management ("Living Agreement") • Support & Capacity Building (IGs) • Scalability to Support Array of Participants (Horizontal/Vertical) • Glossary of TF Terms/Definitions • Modular Approach for TF Elements – IdPs, RPs & ITSPs • Law Enforcement (LE) Use Case: Support for Data Sharing • Federal Government Use Case: Federal Agency as RP (FICAM)

CSDII
Cross Sector Digital Identity Initiative

Detailed Walk-through

Summary Points:

- Model TFs ranged along a continuum from the Descriptive to Prescriptive
- Issues of specificity and applicability at the Descriptive end of the continuum
- Concerns over scalability and legal constraints at the Prescriptive end of the continuum

CSDII
Cross Sector Digital Identity Initiative

Next Steps

- Learn from the gap analysis to develop a detailed outline (core elements and agreements) for the CSDII TF
- Engage InCommon to build from its TF elements and agreements
- Prepare a TF for the CSDII that reflects best practices and meets all requirements

CSDII
Cross Sector Digital Identity Initiative

For More Information

Joseph W. Grubbs, Ph.D.
Enterprise Information Architect
Commonwealth Data Governance
Virginia Information Technologies Agency
Phone: (804) 416-6171
Email: Joseph.Grubbs@vita.virginia.gov