National Strategy for Trusted Identities in Cyberspace (NSTIC)
American Association of Motor Vehicle Administrators (AAMVA) – CSDII Pilot Project
Trust Framework (TF) Gap Analysis

Purpose

The purpose of the gap analysis was to evaluate how selected model Trust Frameworks (TFs) aligned with TF requirements for the CSDII Pilot Project ("Project"). Analysts applied a matrix of the required TF elements as an analytical tool to evaluate the six model TFs, which have been implemented across multiple domains. Highlights from the findings have been provided below, with full tables on the following pages.

Model TFs reviewed in the analysis:

- AAMVA DL/ID Security Framework – Set of requirements, recommendations and standards maintained by AAMVA for use by Motor Vehicle Administrations to ensure drivers license and identification security.
- eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA) – Trust framework established to support the exchange health information and messaging within the Nationwide Health Information Network (NwHIN, now eHealth Exchange).
- InCommon Trust Framework – Trust framework designed to facilitate authentication and identity management for students, faculty, staff and other service providers for institutions of higher education.
- Kantara Initiative Trust Framework – Trust framework developed on a for-profit, subscription basis to enable secure, identity-based, online interactions in a secure environment.
- Open Identity Exchange (OIX)/OITF Model – Set of guidelines and recommended mechanisms (Level of Assurance and Level of Protection) for developing and implementing a trust framework for secure, confidence-based exchange of information.
- CIVICS/IDCubed.org Trust Framework – Model designed by Civics (in partnership with the MIT Media Lab) and IDCubed.org, a private non-profit organization, which outlines the business, legal and technical elements of a trust framework.

Key Findings

The model TFs ranged on a continuum from "descriptive," those setting minimum standards for trust-based information exchanges without actually structuring an exchange, to "prescriptive," those establishing specific agreements, policies, procedures and specifications to support an information exchange. Substantive gaps in alignment with the Project TF requirements were observed along this continuum.

Primary gaps in alignment included the following:

- The more descriptive TFs lacked the level of specificity required for the Project TF; these descriptive TFs may be used as high-level checklists for the Project TF but failed to

provide the necessary business, legal and technical (BLT) provisions for the Project exchange; the Project TF will need to cover the full range of BLT requirements.

- The prescriptive TFs tended to be either excessively domain-centric or failed to take account of the unique legal status of government agencies, particularly state government; issues of sovereignty, statutory authority, liability and grant of authority will need to be fully addressed in the Project TF.

Conclusion

The InCommon TF Model was found to be the most robust, mature and scalable of those reviewed for the Project. Primary strengths of the InCommon TF:

- Addressed the cited concerns relating to legal issues for state government agencies, including sovereignty, statutory authority, liability and grant of authority.
- Provided detailed guidance, agreements and support documentation for structuring an exchange in the ID assurance and management space.
- Established binding BLT requirements for all relevant participant types, including Identity Providers (IdPs), Relying Parties (RPs) and Assurance Providers.
- Featured extensive use-cases demonstrating the types of participants, types of exchanges, operational/functional elements and other dimensions of the exchange.

National Strategy for Trusted Identities in Cyberspace (NSTIC)
American Association of Motor Vehicle Administrators (AAMVA) – CSDII Pilot Project
Trust Framework (TF) Gap Analysis

	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)

Trust | Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
AAMVA DL/ID Security Framework	+ Data element-level verification and validation (§1.3 #9, §1.4 #10, §1.4 #13, §3.3.4, §7.4, Appdx.) + Data (Name) collection, use and maintenance (§3.3.4, § 7.1, Appdx.) + AAMVA DL/ID Personal ID Card Design Specification (§1.4 #12, §3.3.4, 7.3, Appdx.) + Procedures for initial customer ID and validation (§3.3.3, §6.0) + Record & document use, permitted purpose (§3.3.5, §4.6, §7.1, §8.0) + Benefits/ business drivers (§2.0, §3.1) + Business-driven agreement among MVAs (§3.1, §3.3, §4.5) + Business requirements for P&Ps, document issuing systems, and internal controls, Driver License Agreement (DLA) (§3.3.1, §4.2, §4.5, Appdx.)	+ Assumes MVA compliance with applicable law, document use, data sharing (§1.5 All Recs., §3.1, §3.2, §3.3.5, §4.5, §8.3, Appdx.) + Enforcement thru business requirements (§2.0, §3.1, §4.5) + Audit plan (§1.1 #2, §1.2 #5, §3.3.2, §5.1, Appdx.) + Compliance and oversight, internal controls (§3.3.2, §4.4, §5.2) + Risk assessment & management (§1.1 #3, §3.3.5, § 4.2, §4.4, §8.0) + Privacy (§1.1 #4, §4.2, Appdx., §3.3.4, §3.3.5, §4.5, §4.6, §7.1, §7.4, §8.3) + Common set of verifiable resources (§1.3 #8, §3.3.3, §6.2, Appdx.) + Machine-Readable Technology (MRT) (§3.3.5, §8.2, Appdx.) + Restrictions, minimum penalties and sanctions (§3.3.5, §8.1, Appdx.)	+ Electronic verification (w/issuing entity) of DL/ID data elements (§1.3 #9, §3.3.3, §6.3) + Standards for MVA system integrity, interoperability & reciprocity (§2.0, §3.1, §3.3.2, §4.2, §4.5) + Compliance & oversight with adopted standards (§3.3.2, §4.5, §5.2) + System integrity, security & privacy (§4.6)	+ Compliance and implementation support thru FDR employee training (§1.1 #1, §3.3.1, §4.1) + Common definition of "residency" (§1.3 #6, §3.3.3) tied to DL/ID verification (§1.3 #7, §3.3.3, §6.1) + "End of stay" on immigration doc. as expiration date for DL/ID - data element derivation (§1.4 #11, §3.3.4, §7.2, Appdx.) + Horizontal scalability thru reciprocity (§3.1) + Openness enforced thru privacy provisions (§4.6, §7.1) + Limits on disclosure enforced thru privacy provisions (§4.6, 7.1) + Glossary of abbreviations/ acronyms (§9.0) + LE Use Case (§1.5 Rec. #8, data sharing §3.3.5, §8.3, Appdx.)

Trust | Security Framework – Exchange Assessment	Gaps (-) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
AAMVA DL/ID Security Framework	– Does not bind RPs or ITSPs to same set of business requirements as IdPs – Fails to establish governing body (also no granting of authority) or change processes to maintain framework – Does not address participant suspension or termination – Structured as a voluntary agreement rather than a binding contract; inadequate to structure an exchange	– Does not contain necessary set of legal agreements to structure an exchange – Lacks the force of law (i.e., legal contract) to compel participant compliance or performance – Fails to establish P&Ps for dispute resolution – Does not bind RPs or ITSPs to same legal requirements as IdPs – Does not include anti-circumvention provisions (one-off agreements) – Due to scalability issue, fails to assign liability & risk to non-MVA participants – "Thin" assumption of participant compliance with applicable law may be inadequate to meet legal (OAG) scrutiny	– Contains only limited operational/technical components – Fails to clearly establish performance & service specifications or applicable standards – Does not bind RPs or ITSPs to same set of technical requirements as IdPs – Does not address breach notification or related security requirements – Limited specifications for system access policies – Lacks requirements on participant duty to respond to requests – Does not address treatment of test data v. production data; future use of data	– Does not support or anticipate non-MVA participants, except for LE (horizontal/vertical scalability) – Does not bind RPs or ITSPs to same set of training requirements as IdPs – Lacks governance provisions to ensure a "living" framework

Trust | Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)	+ Definitions of permitted purpose (§1.jj; §3; §5.01-5.03) + Governing body (§4) & change processes (§10.03; §11.03) + Operating policies & procedures (§11; Appdx.; change process in §11.03) + Security, privacy & confidentiality (§7; §8; §14) + Suspension & termination (§19) + Data elements & data classification (attribute level/PII) (§1.v; §1.w; §1.kk) + Expectations of performance (§12)	+ Definition/compliance w/ applicable law (§1.a; §15.11; §23.01; Appdx.) + Legal agreements (set) for exchange structure (recitals; §1.ee; §3.01; §23.07) + Security, privacy & consent (§14) + Liability (§18) + Representations & warranties (§15; disclaimers in §17) + Grant of authority (§4.03) + Dispute resolution (§21; Appdx.) + Authorizations for data exchange (§12; §13) + Open disclosure & anti-circumvention (§15; §23.04; §23.07) + Confidential participant information (§16) + Audit (§9) + Accountability & compliance (§10.01; 11.01; §15.03; §15.06)	+ Performance & service specifications (§10; Appdx.; change process in §10.03) + Security, privacy & confidentiality (§7; §8; §14) + Breach notification (§14.03) + System access (§6) + Provisions for future use of data (§5.02) + Expectations of participants (§12) + Duty of response by participants (§13) + Onboarding, testing & certification (§10.01) + Handling of test data v. production data (§15.07)	+ Openness & transparency (overview; recitals) + TF lifecycle management ("living agreement") (overview; §4; §10.03; §11.03) + Scalability to support array of participants (horizontal/vertical) (participant types defined in §1; expectations in §12.02; duties in §13) + Glossary of TF terms/definitions (§1) + Modular approach for different participant types (types defined in §1; expectations in §12.02; duties in §13; warranties in §15)

Trust | Security Framework – Exchange Assessment	Gaps (-) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)	– Definition of "permitted purpose" assumes all participants will exchange same type of data/message content; no distinction between participant types (IdPs; RPs; ITSPs) – Governing body not established in statute/ regulations may have limited capacity to issue binding actions – Legal status of TF may be too limited to bind government agencies to operational P&Ps – Governing body action to suspend or terminate may be interpreted as a government agency ceding its statutory authority – Assumes transmittal of a standardized "document" (HL7 CCD) and message content; does not specify down to the attribute level	– Definition of "applicable law" would need to be expanded to cover required data elements and domains – Uncertain whether state agencies would have legal ability to execute TF agreements, and if so at what level (Agency head? Secretariat?) – Assignment of liability, representations and warranties, as written, would be barriers for state agencies – Grant of authority to governing body would not be possible for state agencies (sovereignty) – Audit, compliance and dispute resolution requirements may be interpreted as a government agency ceding its statutory/ regulatory authority – Does not provide guidance on risk analysis or management	– Regulations governing security, privacy & confidentiality differ based on government agency levels and domains; TF needs to address (or at least take into account) – Breach notification and other technical requirements would need to be reconciled with applicable statutes/regulations – Expectations for participants may be interpreted as a government agency ceding its statutory/ regulatory authority	– Limited scalability outside of the health IT/HIPAA domain; requires expanded scope of applicable law and participant types (IdPs; RPs; ITSPs) – Acts as a blanket TF under which each participant must fully execute/comply or forfeit participation; no modular approach for different participant types (IdPs; RPs; ITSPs) – Training and implementation support (IGs) left up to individual participants or vendors; disparate mechanisms – Contains only general references to use cases and other business elements

Trust | Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
InCommon Trust Framework	+ Definitions of permitted purpose (ICPOP; IAS; limits on use of ID information in PA §9) + Governing body & change processes ICBL; ICPP; ICPOP; PA §17) + Operating policies & procedures (ICBP; ICPP;ICPOP) + Security, privacy & confidentiality (PA §6, §9; ICPOP) + Suspension & termination (PA §5.b, §5.c; ICBL) + Data elements & data classification (attribute level/PII) (IAS; FTG; PA §6.b) + Expectations of performance (ICBP; PA §6, §7) + Use cases and examples (InCommon Website; ICBP; Participants)	+ Definition/compliance w/ applicable law (PA §15) + Legal agreements (set) for exchange structure (ICB; ICPP; PA §6, §7.b) + Security, privacy & consent (PA §6, §9) + Liability (PA §11, includes disclaimer & limitations) + Representations & warranties (addressed in PA §7.b) + Grant of authority to executive (PA §18) + Dispute resolution process (PA §10; ICBL §5) + Authorizations for data exchange (PA §18) + Open disclosure & anti-circumvention (PA §14, §16) + Confidential participant information (PA §8, §9) + Audit (IAF) + Accountability & compliance (PA §15; IAF)	+ Performance & service specifications (FTG; ICBP; PA §6, §7) + Security, privacy & confidentiality (ICBP; ICPOP) + Breach notification (PA and addenda; ICPOP) + System access (ICBP) + Provisions for future use of data (ICPOP) + Expectations of participants (ICBP; PA §6, §7) + Duty of response by participants (ICBP; PA §6, §7) + Onboarding, testing & certification (ICBP) + Handling of test data v. production data (ICPOP)	+ Openness & transparency (ICBP; ICBL) + TF lifecycle management ("living agreement") (ICBL; ICBP; PA §17) + Implementation support (ICBP; ICPOP) + Scalability to support array of participants (horizontal/vertical) (participant types defined in Join §1, Participants; ICBP) + Glossary of TF terms/definitions (InCommon Website) + Modular approach for different participant types (ICB; Participants)

Join=www.incommon.org/join.html; Participants= www.incommon.org/participants/
FTG=InCommon Federated Technical Guide; ICBP=InCommon Basics and Participating in InCommon, Jan. 21, 2011
ICPP=InCommon Policies and Practices; ICPOP=InCommon Participant Operational Practices; ICBL=InCommon Bylaws
PA=InCommon Participation Agreement; IAS=InCommon Attribute Summary; IAF=InCommon Assurance Framework

Trust | Security Framework – Exchange Assessment	Summary of Alignment with Required Elements & Provisions for CSDII Pilot Project
InCommon Trust Framework	The analysis failed to identify any substantive gaps in the InCommon TF Model, which ranked as the most robust, mature and scalable of those reviewed for the CSDII Pilot Project. Primary strengths of the InCommon TF: • Addressed the cited concerns relating to legal issues for state government agencies, including sovereignty, statutory authority, liability and grant of authority. • Provided detailed guidance, agreements and support documentation for structuring an exchange in the ID assurance and management space. • Established binding BLT requirements for all relevant participant types, including Identity Providers (IdPs), Relying Parties (RPs) and Assurance Providers. • Featured extensive use-cases demonstrating the types of participants, types of exchanges, operational/functional elements and other dimensions of the exchange.

Trust | Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Kantara Initiative Trust Framework	+ Definition of permitted purpose (KTR MTAU) + Governing body (BL §4; OP §2) & change/ amendment processes (BL §12; OP §9; MA §3) + Operating policies & procedures (OP) + Security, privacy & confidentiality (AP; MA) + Suspension & termination (MA §2; BL §8.11; KTR MTAU) + Data elements & data classification (KTR; KIC) + Expectations of performance (AP; KTR MTAU; KIC) + Use cases (Working groups for business cases-trusted federations)	+ Definition/identification of applicable law (KTR MTAU; see also "Governing law and jurisdiction" provision in KTR MTAU) + Legal agreement for exchange structure (MA) + Security, privacy & consent provisions + Liability (KTR MTAU) + Warranty (KTR MTAU) + Grant of authority (MA) + Authorizations for data requests by participant + Open disclosure & anti-circumvention (Other agreements in KTR MTAU) + Confidential participant information (Options set in IPRP; IPRP Art. 3) + Accountability & compliance (w/ antitrust laws in BL §17; MA)	+ Performance & service specifications (AP; KTR/KTV; KTR MTAU; KIC; Member protection & treatment in IPRP) + Security, privacy & confidentiality (AP; MA) + Technical certification & testing (AP; KIC) + Standards for technical & operational interoperability (KTR; MA goal #3; #7; KIC)	+ Open & transparent governance model (MA goals #3, #4; op; BL §3) + TF lifecycle management (MA goals #4, #6) + Support & capacity building (IGs) + Scalability to support array of participants (horizontal/vertical) (member types BL §8) + TF definitions (BL §1; OP §1; IPRP Art. 2)

BL=Bylaws; IPRP=Intellectual Property Rights Policies; MA=Member Agreement; OP=Operating Procedures
KTR=Kantara Trust Registry; KTV=KTR Trust Validation; KTR MTAU=Metadata Terms of Access & Use; KIC= Kantara Interoperability Cert.-SAML, OATH, etc.
AP= Assurance Programs; Identity Assurance Accreditation & Approval and Interoperability Certification Programs

Trust | Security Framework – Exchange Assessment	Gaps (-) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Kantara Initiative Trust Framework	– Permitted purposes limited to assurance & interoperability dimensions; "thin" on provisions for RP use – Governance model & operational procedures do not structure an actual exchange rather designed to be used by members for their exchanges – TF focuses on IdPs, Credential Service Providers & Assurance Providers; provisions limited for RPs	– TF contains a well established legal framework for membership & governance but does not structure an actual exchange – "Thin" statements re compliance with applicable law – TF limited to setting requirements for member use of technical and operational assurance programs for their own exchanges – TF does not fully address audit requirements – Legal provisions contain only limited provisions for RPs; main focus on IdPs, Credential Service Providers & Assurance Providers – Bylaws and operational policies do not provide for dispute resolution	– Performance, service and other technical specifications set for IdPs, Credential Service Providers & Assurance Providers; limited coverage for RPs – RPs play narrow role as inputs on IdP and assurance requirements – Specifications do not cover an actual exchange but designed to support member use in their exchanges – Certification & testing but "thin" coverage for RPs or other potential participant/member types	– Governance model sets up for a "living" TF thru an extended lifecycle, with horizontal and vertical scalability; however, limited on RPs and other potential participant/member types

Trust | Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Open Identity Exchange (OIX)/OITF Model	+ Definitions of permitted purpose (OITF §III.B, §III.C, §V) + Governing body & change processes (OIX; OITF §III.C) + Operating policies & procedures (OIX; OITF §II, §III.B, §III.C) + Security, privacy & confidentiality (OIX; OITF §III.A, §V) + Suspension & termination (OITF §III.C) + Data elements & data classification (attribute level/PII) (OIX; OITF §III.A, §III.B) + Expectations of performance (OIX; OITF §II, §III.C) + Use cases for agreement, transaction & participant types (OITF §I, §III; OIX)	+ Compliance w/ applicable law (OIX; OITF §V) + Legal agreements (set) for exchange structure (OIX; OITF §II, §III.C) + Security, privacy & consent (OIX; OITF §III.A) + Liability, representations & warranties (OITF §III.C) + Grant of authority (OIX; OITF §III.C) + Dispute resolution (OITF §II, §III.C, §V) + Authorizations for data exchange (OIX; OITF §III.A) + Anti-circumvention & open disclosure (OITF §V) + Audit (OIX; OITF §II, §III.B, §V) + Accountability & compliance (OIX; OITF §II, §V)	+ Performance & service specifications (OIX; OITF §II, §III.A, §III.B) + Security, privacy & confidentiality (OIX; OITF §III.A; §V) + Expectations of participants (OIX; OITF §III.A, §III.B, §III.C) + Onboarding, testing & certification (OIX; OITF §II, §III.B)	+ Openness & transparency (OIX; OITF §I; statement in OITF §V, §VI) + TF lifecycle management (OIX; OITF §II) + Scalability to support array of participants (horizontal/vertical) (OITF §II, §III.C, §IV) + High-level definitions (OITF §I) + Modular approach for different participant types (OIX; OITF §II, §III.C) + Use cases & examples of TFs (OITF §IV)

OITF=The Open Identity Trust Framework (OITF) Model, March 2010
OIX=Open Identity Exchange Trust Framework Requirements and Guidelines v. 1 (Draft 2)

Trust | Security Framework – Exchange Assessment	Gaps (-) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Open Identity Exchange (OIX)/OITF Model	– Highlights primary business-related TF elements and requirements; however, fails to provide level of specificity needed for structuring an exchange – Reads more like a high-level checklist for TF elements & provisions rather than an actual TF (That said, OITF will be useful as a checklist to ensure alignment for the CSDII TF; also, OITF provides several use cases and examples of an ID exchange)	– Outlines primary legal TF elements and requirements; however, fails to provide documents/agreements needed for structuring an exchange – Provides a checklist for the set of necessary legal agreements for the TF and a high-level identification of the issues to be covered in the agreements (i.e., grant of authority, liability, warranties, authorization, etc.); however, no "concrete" examples or agreement models – States the requirement for participants to comply with applicable law but does not cite governing statutes, laws and regulations for an actual exchange	– Identifies primary technical elements and requirements to be covered in a TF; however, fails to provide level of specificity needed for structuring an exchange – Provides a checklist for the set of necessary technical specifications, certification and testing of those specifications; however, OITF stops as simply identifying the specifications and LOA certification without giving detailed content provisions	– Addresses the necessary principles of openness, transparency, scalability and full lifecycle management; however, as with the other domains fails to provide the degree of specificity needed for structuring an exchange

Trust | Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
CIVICS/IDCubed.org Trust Framework	+ Definitions of permitted purpose (ID3LA §3, §5.2 §5.3; CTA §2.4.2.5) + Governing body & change processes (ID3LA §9.8) + Operating policies & procedures (ID3LA) + Security, privacy & confidentiality (ID3LA §6, §17; CTA §2.4.2.7) + Suspension & termination (ID3LA §4.4, §11) + Data elements & data classification (attribute level/PII) (ID3LA §3, §5.2 §5.3; CTA §2.4.2.2.3.1) + Expectations of performance (ID3LA §4, §9; CTA §2.4.2.2.3.1)	+ Compliance w/ applicable law (ID3LA §9.7, §18, §24.8) + Legal agreements (set) for exchange structure (ID3LA; CTA §2.2) + Security, privacy & consent (ID3LA §6, §17; CTA §2.4.2.7) + Liability (limitations ID3LA §13.2; CTA §2.5.2) + Representations & warranties (ID3LA §19) + Grant of authority (ID3LA §24; CTA §2.2.1) + Dispute resolution (ID3LA §21) + Authorizations for data exchange (§12; §13) + Non-exclusivity (ID3LA §5.4, assignment ID3LA §24.3) + Confidential participant information (ID3LA §7, §10, §17; CTA §2.3.1.1) + Audit (ID3LA §16.2; CTA §2.4.2.8) + Accountability & compliance (ID3LA §16.3, §18; CTA §2.4.2.8)	+ Performance & service specifications (ID3LA §9) + Security, privacy & confidentiality (ID3LA §6, §17; CTA §2.4.2.7) + Breach notification (ID3LA §17.3) + System access (ID3LA §7.2) + Provisions for future use of data/services (ID3LA §3.8) + Expectations of participants (ID3LA §4, §9; CTA §2.4.2.2.3.1) + Duty of response by participants (ID3LA §4, §9; CTA §2.4.2.2.3.1) + Onboarding, testing & certification (ID3LA §4; CTA §1.3.1)	+ Openness & transparency (ID3LA §1; CTA §2.4.2.1) + TF lifecycle management (ID3LA §1) + Scalability to support array of participants (ID3LA §1, participant types defined in Schedule 2; CTA §1.2) + Glossary of TF terms/definitions (ID3LA Schedule 2; CTF Addenda 2) + Modular approach for different participant types (ID3LA §1, participant types defined in Schedule 2; CTA §1.2)

ID3LA= IDCubed.org Legal Agreement for Trust Framework Data Store, Nov. 8, 2012
CTF=Civics Model Trust Framework for Person Data, Feb. 22, 2012

Trust | Security Framework – Exchange Assessment	Gaps (-) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
CIVICS/IDCubed.org Trust Framework	– CIVICS Model TF contains the high-level elements & provisions to support business-related requirements for an exchange; however, the model has not achieved a level of maturity needed to fully support the CDSII Pilot Project – Additional model documentation & examples, particularly of the Commonwealth of Massachusetts, would be needed to make a final determination – Model does not fully address data elements & permitted purposes	– CIVICS Model TF features legal agreements to support an exchange; however, it is unclear whether the model's legal framework would be adequate to cover state agency participants – For future analysis, it would be beneficial to have examples of other implementations, particularly the Commonwealth of Massachusetts procurement TF (referenced during presentation on 2/14/2013)	– Model TF does not provide level of specificity in key technical areas, including performance & service specifications; onboarding, testing & certification; breach notification & system security	– Model could be supported more fully by use cases, examples of participants & transactions, & implementation guides