Framework for State/Local ICT Policy: IOT, Cloud, Block Chain, etc.

Michael A. Aisenberg, Esq.

December 2017

© Michael A. Aisenberg 2017
Premise: Policy is Failing at Federal Level

- 20 years of little Federal legislative consensus on ICT
- Policy by Executive Order is not good policy
  - EOs Can NOT address S/L/T Interests
- In ICT, $65 billion/year at stake in the states
- Citizens are left without a remedy when injured:
  - Slow/absent Federal policy not keeping pace with exploding presence of ICT in Critical Infrastructures, local businesses, homes and workplace

© Michael A. Aisenberg 2017
5 Areas Ripe for State Action

1. Undo pre-emption of civil suits for regulated IOT devices
2. Improve action against fraud
3. Modernize contracting for technology
4. Share information across states
5. Harmonize state approaches thru a Uniform State statute (ULC/NCCUSL)
Reverse existing preemption of state civil jurisdiction for IOT injuries

• **Present law:** Federal regulation preempts state court jurisdiction
  • citizens injured by an IOT device subject to Federal regulation may not sue vendor in state court
    – Connected medical devices (FDA)
    – Unmanned vehicles and aircraft (drones) (NHTSA, FAA)
  • Unfair when Federal regulatory agency review does not go to technology flaws: bad software, counterfeit chips, failed network security

• **Solution:** state statute to grant jurisdiction to state courts to hear suits against vendors

(C) Michael A. Aisenberg 2017
Improve contracting for technology devices, software, services

- "ICT" is one of 3 top purchases by localities: $65 billion in 2016
- States lack expertise of Federal government, which spends $100 billion+ annually in DoD alone
  - Fed ICT acquisition has extensive safety net procedures
- Revise state acquisition model to add technology expertise/best practices throughout life cycle: procurement, use.

(C) Michael A. Aisenberg 2017
Inspector General (IG)

• Technology acquisition is complex: it goes wrong even when well planned/managed

• 90+ State/county/local jurisdictions have established Inspectors General to address fraud, waste, abuse and protect taxpayers

• ICT is #1, 2, or 3 in SLT budgets each year
  – Law enforcement, schools, transportation agencies buy billions nationwide

• IGs have expertise; investigate, bring cases, pursue bad vendors
Fusion Centers for IOT Flaw Information Sharing

- Joint centers managed by state agencies (AG, C/J) with DoJ, DEA, DHS:
  - 79 nationwide-Primary foci: C/I, drug interdiction, C/T
- Extensive information sharing network
  - Proposal: extend role to information sharing on flaws in IT (IOT devices, software, security))
  - Bundle with DHS SLTT Security Clearance Initiative
    - grant security clearances to state Chief Information Officers (CIOs) and Chief Information Security Officers (CISO)
    - Shares actionable classified and sensitive information about current and recent cyber incidents and threats
Paths Forward

• States & localities:
  – Introduce, debate and pass legislation to grant jurisdiction to local courts on ICT flaws
  – Improve ICT acquisition process
  – Establish Inspectors General
  – Use Fusion Centers to share ICT/IoT alerts

• States acting together
  – Use Uniform Law Commission (ULC) to develop Model State Act on civil jurisdiction, information sharing