

---

# State Privacy Officer Update

March 2022

---

# State Privacy Officer Responsibilities

- Analyze and report on government privacy practices
- Provide educational and training materials
- Identify privacy practices that pose the greatest risk to individual privacy and prioritize those privacy practices for review
- Respond to requests from individuals to review a designated government entity's privacy practice
- Make privacy recommendations to the State Legislature

---

# Vision

Provide legal, practical, and ethical solutions to designated governmental entities to protect citizen privacy and increase public trust.

\*Technology isn't going to solve this. Coaching is critical.

---

# Scope

- **262,860 employees**
- **1,147 designated government entities:**
  - Local and Special Service District 391
  - Local Education Agency 152
  - City 146
  - Town and townships 108
  - Redevelopment Agency/Project Area 89
  - State of Utah (depts/comp units/etc.) 67
  - Interlocal 62
  - Conservation District 38
  - County 29
  - Housing 19
  - Institution of Higher Education 18
  - Misc. 28

# My Plan



Measure Baseline

Build Relationships

Deliver Resources

---

# Privacy Maturity Survey

- All Local Education Agencies, 153
- All Counties, 29
- All other designated government entities with 50 or more employees, 168

\*53% response rate

## Privacy Program Criteria

Maturity Level	Contracts with Clients & Partners	Infrastructure & Systems Management	Policy Documentation	Privacy Awareness & Training	Privacy Budget	Privacy Function	Privacy Incident Management	Privacy Personnel	Risk Assessment
0	Contracts do not address privacy	Procurement of IT-related products & services do not address privacy	There are no documented privacy policies	Contents of privacy policies are never communicated with personnel	There is no budget specifically allocated to privacy purposes	There is no assigned privacy office or function	No was to respond to suspected incidents	No one person with a job description of a privacy officer	Project plans & acquisition of IT-related products do not address privacy
1	Confidentiality clauses are included in contracts, but compliance cannot be monitored	Project and IT managers occasionally address privacy in plans & system-development	Multiple, inconsistent policies, or policies that do not address all privacy principles	Some contents of privacy policies are communicated to some personnel	No specific budget, but privacy dollars are spent ad hoc as add-ons to other projects	One person assigned privacy responsibilities serves as the privacy function	Some personnel have knowledge and skills to respond to suspected incidents	At least one person is assigned privacy responsibility, but time commitment exceeds the person's availability	Project & IT managers occasionally address privacy in project plans & system development
2	Personnel review contracts for consistency with privacy policies	Policies require that IT products, services, and system development address privacy	Policies address all privacy principles, and are displayed on relevant websites.	Privacy policies are communicated annually to personnel who encounter PII	Specific budget sufficient to cover basic travel & subscriptions, and modest amount for special projects	Privacy function is identified in org charts, reflecting sustained commitment	Privacy incidents have been effectively resolved, but at most only high-level policy or procedures are documented	At least one person devoted exclusively to privacy, with sufficient staff assistance	Policies require acquisition of IT-related products & services address privacy
3	Standard contractual clauses are in place, and compliance can be monitored	Detailed checklists & procedruers are used to insure compliance with policies	Policies address all privacy principles, are publicly displayed, and details for implementation are included	Privacy policies are communicated annually to personnel who encounter PII and are provided role-based training	Specific budget that includes enough money to accomplish most privacy objectives	An executive committee member is formally assigned to be privacy champion, and an annual report is presented to board	Personnel have detailed roles and responsibilities, and detailed policies & procedures are maintained	Privacy staff have clearly defined job descriptions that require certification as CIPP, including at least one with a leadership title, and enough staff to meet most privacy objectives	Detailed checklists, procedures and assigned personnel to ensure all IT-related projects are compliant with privacy policies
4	Standard privacy & security clauses and internal compliance are measured annually	Compliance with privacy policies of IT products and services are measured and routinely tested	Business operations, processes, etc. are reviewed annually, and are updated as needed	Personnel comprehension of, and compliance with privacy policies is measured annually	A "Balanced Privacy Scorecard" or other approach used to determine a budget sufficient to cover all objectives	The privacy function is placed in a particular dept to support its strategy, and has direct access to Executive Committee	Suspected incidents are routinely measured & tested for privacy compliance, improvements are made based on this	Privacy staff have clearly defined job descriptions that require certification as CIPP, a Chief Privacy Officer, and enough staff to meet all privacy objectives	Information-related products and services are routinely measured and tested for compliance with privacy policies
5	Controls in place to prevent adoption of privacy & security commitments that cannot be kept	Controls in place to ensure IT products and services are compliant with policy and procedure	Policies & standards are compared annually to others, and have achieved "best practices" status	Policy compliance is compared annually to others, and have achieved "best practices" status	Privacy function funds are exceeded by privacy dollars spent elsewhere in the organization	The head of the privacy function has direct access to leadership and is a part of business strategy decision-making	All incidents are resolved within 30 days	Privacy objectives are in the job descriptions of all personnel who access PII	Controls in place to prevent new IT-related products and services from being deployed without being compliant with privacy policies

## Average Score by Privacy Topic





## **Top 10**

8 Local Education  
Agencies (LEAs)

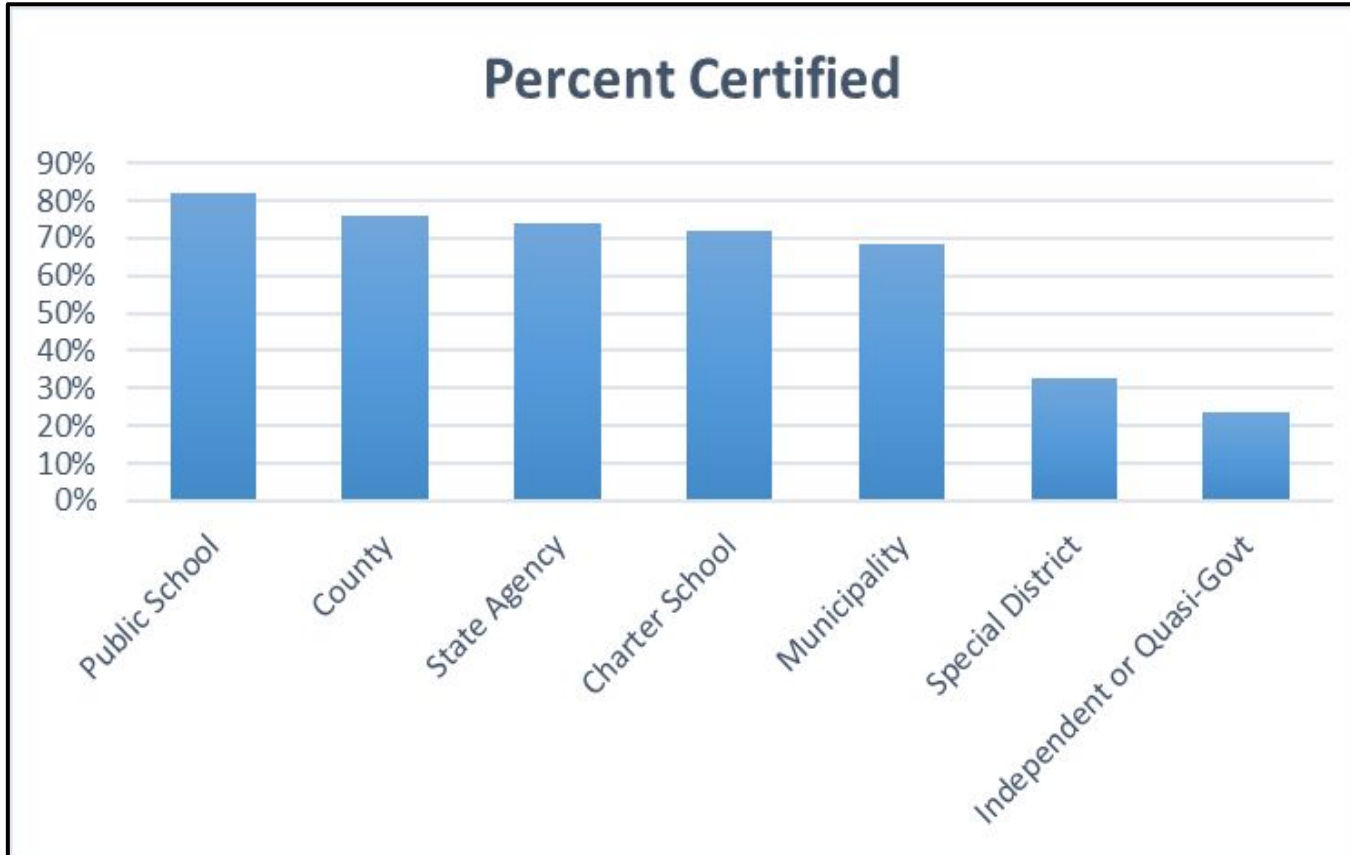
2 Behavioral  
Health Facilities

## **Bottom 10**

4 Counties

6 Cities

## 63G-2-108: Record's Officer annual certification requirement:





# Next Steps

Spring 2022

- Measure privacy maturing of medium and small designated government entities
- Develop training materials

Summer 2022

- Train large designated government entities
- Hire additional privacy FTE

Fall 2022

- Legislative Report
- Host the Utah Privacy Conference for specific designated government entities