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

- Infrastructure and Systems Management
- Policy Documentation
- Privacy Awareness and Training
- Risk Assessment
- Clients and Partner Contracts
- Privacy Incident Management
- Privacy Function
- Privacy Personnel
- Privacy Budget

Scores range from 0 to 3.
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