# Agenda - Digital Privacy Advisory Taskforce

**Date**: February. 13, 2020 **Time:** 2:30 P.M. **Location:** City Hall, T-1752 17th Floor

**Goal/Purpose of the Digital Privacy Advisory Taskforce Meeting:**
1) Clarify roles and responsibilities of the Taskforce
2) Leverage Taskforce expertise to inform the City's development of a governance model for digital privacy

**A. Introductions**

**B. Update from Deputy City Manager**

**C. Digital Privacy Workplan Status Update**

**D. Co-Create and Design First Draft Governance Model Prototype**

1. NIST, GDPR, and Seattle models
2. Facilitated Activity: Building Draft Prototype for San Jose
3. Identify Gaps & Priority Areas for Governance

**E. Next Steps**

**Privacy Advisory Taskforce Members:**

- Victor Sin, Chair of the Santa Clara Valley Chapter, ACLU of Northern California
- Roxana Marachi, San Jose Silicon Valley NAACP
- Heather Patterson, Senior Research Scientist, Intel Labs & Privacy Scholar at NYU
- Harvey Jang, Vice President & Chief Privacy Officer, Cisco
- Bob Lim, Vice President Information Technology & Chief Information Officer, San José State University
- Irina Raicu, Director, Internet Ethics, Markkula Center for Applied Ethics, Santa Clara University
- James Randol, Retired San José Police Department Captain
- Mike Shapiro, Chief Privacy Officer, Santa Clara County

Contact: Sarah Papazoglakis, Senior Privacy Policy Analyst, Office of Civic Innovation and Digital Strategy, (408) 535-8196.
10/3/2019

**Attachments:**

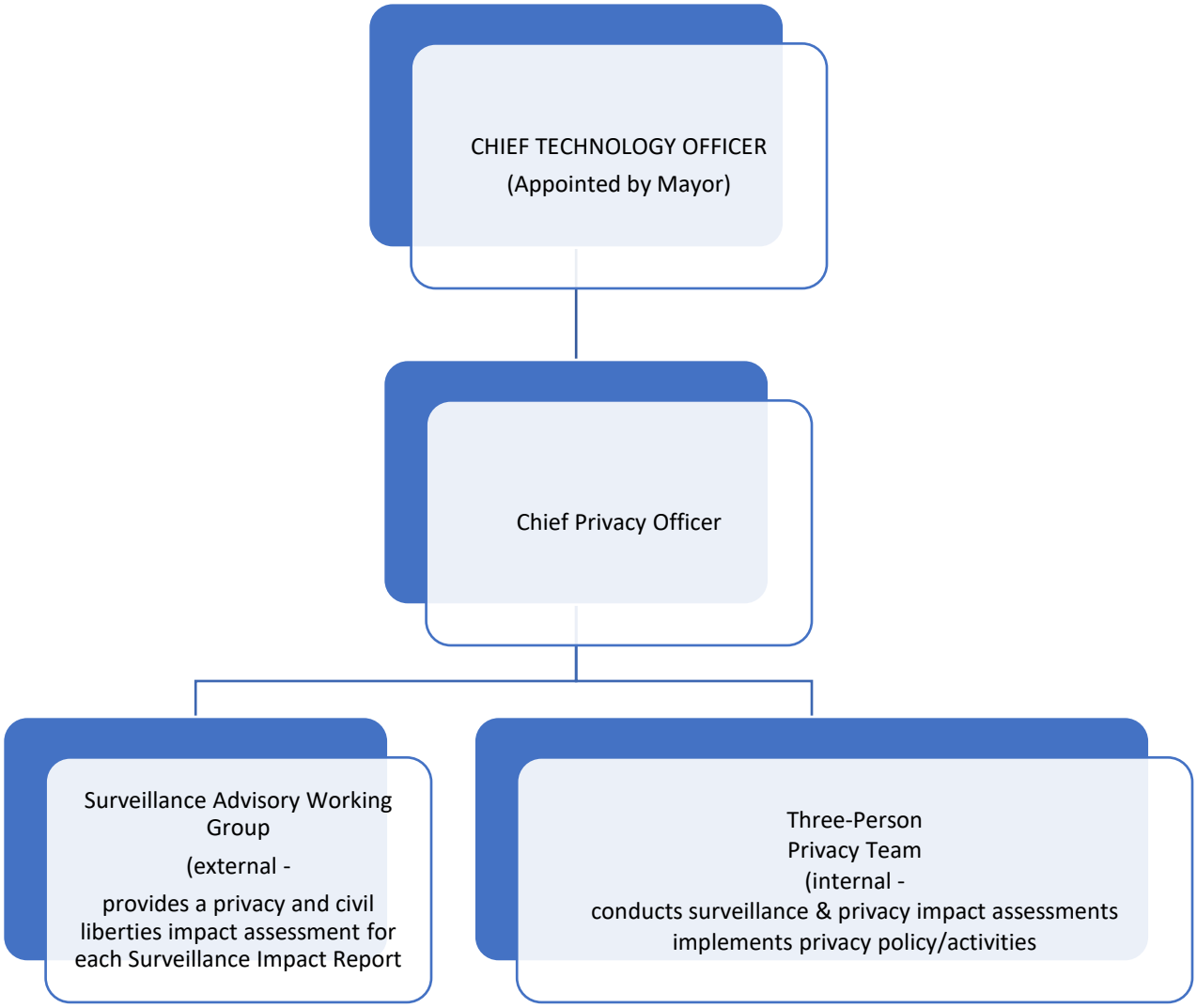
1) NIST & Seattle Frameworks
2) GDPR_CIPL Accountability Wheel

Contact: Sarah Papazoglakis, Senior Privacy Policy Analyst, Office of Civic Innovation and Digital Strategy, (408) 535-8196.
10/3/2019

**National Institute of Standards and Technology (NIST)**
**Privacy Framework: Governance**

| | Function | Category | Subcategory |
|---|---|---|---|
| | **GOVERN-P (GV-P):** Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. | **Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. | **GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated. |
| | | | **GV.PO-P2:** Processes to instill organizational privacy values within system/product/service development and operations are established and in place. |
| | | | **GV.PO-P3:** Roles and responsibilities for the workforce are established with respect to privacy. |
| | | | **GV.PO-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners). |
| | | | **GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed. |
| | | | **GV.PO-P6:** Governance and risk management policies, processes, and procedures address privacy risks. |
| | | **Monitoring and Review (GV.MT-P):** The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk. | **GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change. |
| | | | **GV.MT-P2:** Privacy values, policies, and training are reviewed and any updates are communicated. |
| | | | **GV.MT-P3:** Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place. |
| | | | **GV.MT-P4:** Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place. |
| | | | **GV.MT-P5:** Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events). |
| | | | **GV.MT-P6:** Policies, processes, and procedures incorporate lessons learned from problematic data actions. |
| | | | **GV.MT-P7:** Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place. |

**City of Seattle**
**Privacy Team Structure**



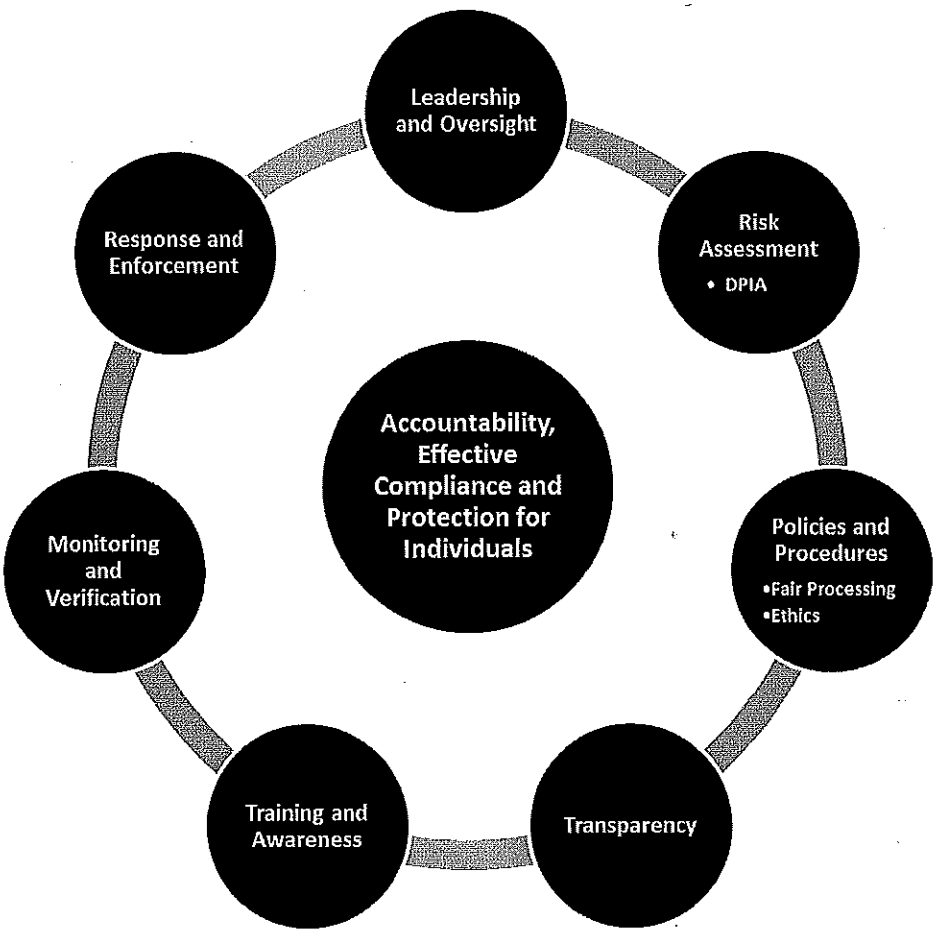



*Figure 1 – CIPL "Accountability Wheel" – Universal Elements of Accountability*

| Accountability Element: | The Accountable Organisation... |
|---|---|
| **Leadership and Oversight** | Ensures appropriate data privacy governance, accountability, oversight, reporting, and buy-in from mid-level and top-level management, including appointing appropriate personnel (e.g., DPO or DPO Team, senior level privacy executives and data governance staff) to oversee the organisation's privacy and accountability program and report to senior management and the board. |
| **Risk Assessment** | At program level, periodically assesses its privacy program and its relevance in light of changes in business models, risk, law, technology and other external and internal factors. At product, service and project level, implements controls to identify, understand and mitigate risks to individuals and organisations. In case of a data breach incident, assesses the potential risks to the rights and freedoms of individuals to mitigate the risks and perform the relevant notifications to the DPA and the data subjects. |

| | |
|---|---|
| **Policies and Procedures** | Builds and maintains written data privacy policies and procedures that reflect applicable laws, regulations, industry standards and organisational values and goals and implements mechanisms to operationalise them throughout the organisation. This includes policies and procedures to ensure fair processing and ethical considerations. |
| **Transparency** | Communicates to individuals critical information about its data privacy program, procedures and protections, as well as the benefits and/or potential risks of data processing and information about individual rights through easily accessible means (e.g., privacy notices, policies and transparency tools such as dashboards and portals). Communicates and engages with relevant data privacy regulators about its privacy program. |
| **Training and Awareness** | Ensures ongoing training and communication to employees, contractors and others who handle data processed by the organisation about the privacy program, its objectives and controls. |
| **Monitoring and Verification** | Monitors ongoing internal compliance with the program, policies and procedures and establishes procedures for regular self-assessments, internal audits and in some instances external audit or certifications. |
| **Response and Enforcement** | Puts in place appropriate procedures for responding to inquiries, complaints, data protection breaches and internal non-compliance. Enforces against internal non-compliance with the program, rules and controls. Cooperates with third-party certification bodies, Accountability Agents, and data privacy regulators in investigations and enforcement actions. |

*Table 1 – Organisational measures to implement the elements of accountability*