From: Classen, Victoria <Victoria.Classen@coloradosprings.gov>
Sent: Friday, October 25, 2019 11:19 AM
To: privacyframework <privacyframework@nist.gov>
Subject: 2019.10.22 NIST Privacy Framework

Ms MacFarland,

On behalf of the Association of Local Government Auditors (ALGA), please find the attached comments to the NIST Privacy Framework.

Vickie Classen,

Chair, ALGA Professional Issues Committee

Vickie Classen CPA, CIA, CGAP, CGMA, PMP | Audit Supervisor | City of Colorado Springs

107 N Nevada #205 MC 1542 | Colorado Springs, CO 80901-1575

719.385.5692 | Victoria.Classen@ColoradoSprings.Gov

Association of Local Government Auditors

October 24, 2019

Katie MacFarland,
National Institute of Standards and Technology,
100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899

Re: NIST Privacy Framework: Preliminary Draft Comments

Dear Ms. MacFarland,

The Association of Local Government Auditors (ALGA) appreciates the opportunity to respond to NIST Privacy Framework: Preliminary Draft. ALGA represents 272 audit organizations comprising more than 2,200 individuals. This topic is of interest to our members, and we encourage individual audit organizations and members to comment independently should they choose to do so.

We have reviewed the proposed Draft. Overall, we believe it provides useful guidance to help organizations and auditors to assess and address privacy concerns when developing products, services, or activities which could risk an individual's personal information. As voluntary guidance, we believe it could be used as criteria for auditors analyzing risk related to privacy. Our comments are below in bold type in the question and answer format that you requested in the Draft.

Does this preliminary draft: adequately define outcomes that:

- *cover existing practices;*
  - **The suggested approach to risk-based creation of the Current Profile should encourage organizations to methodically define their existing practices.**
- *strengthen individuals' privacy protection;*
- *enable effective organizational use;*
  - **The description of problems for individuals was refreshingly simple and straightforward. Using problems as a generic means to convey the complex issues faced with privacy concerns should help organizations focus on impacts to their users. However the wording on line 239 related to "problematic data action", seemed weak and may not provide enough context to explain how to assess impacts. Perhaps adding in some examples of what the goal is for this step would be helpful.**

MEMBER SERVICES

449 Lewis Hargett Circle
Suite 290
Lexington, KY 40503
Phone: (859) 276-0686
Fax: (859) 278-0507
www.algaonline.org

- *support enterprise mission/business objectives;*
- *and facilitate compliance with applicable laws or regulations;*
    - **We agree that adoption of the Framework should help organizations make effective use, support enterprise mission/business objectives and facilitate compliance with laws and regulations.**
    - **The Hypothetical Use Case Profiles in the Supplemental Materials were especially useful to improve understanding and use of the Privacy Framework, however links to these materials were only available through the web page for the Working Draft as related Materials. We suggest adding them as an Appendix or inserting a link from Section 3.0 How to Use the Framework to these supplemental materials could improve understanding and adoption.**
- *appropriately integrate privacy risk into organizational risk;*
- *provide guidance about privacy risk management practices at the right level of specificity;*
    - **Beginning with Section 2.1 The Core, the description of the Framework and its relationship between Functions, Categories, Sub categories, Current Profile and Target Profile was useful and comprehensive, however Table 2 of Appendix A, was easier to understand. The embedded links in table 2 to definitions were very helpful to the reader. Consider adding in an embedded link in Section 2.1 to Appendix A to give readers direct access to a more thorough explanation and examples.**
- *adequately define the relationship between privacy and cybersecurity risk;*
    - **The diagrams on page 6 and page 19, combined with the color coding in Table 1 were good depictions of the interaction and difference between the privacy and cybersecurity frameworks.**
- *provide the capability for those in different organizational roles such as senior executives and boards of directors, legal, compliance, security, and information technology or operations to understand privacy risks and mitigations at the appropriate level of detail;*
- *provide sufficient guidance and resources to aid organizations of all sizes to build and maintain a privacy risk management program while maintaining flexibility; and*
    - **Appendix D, along with the Privacy Risk Assessment Methodology (PRAM), provides a clear, useful methodology for assessing privacy risks. The PRAM approach aligns well with auditing risk assessments and should be a useful tool for auditors to assess their organizations' management of privacy. Because Appendix D represents Function Identify-P, which is one of the 5 foundational core areas, consider moving the entire appendix into the main document. If the desire is to keep the main document short, we suggest adding more emphasis to point the reader to Appendix D.**
- *enable cost-effective implementation?*
    - **The use cases mentioned above and section 3.3 – 3.5 were most helpful in explaining how the Framework should be implemented to benefit an organization, including defining specific roles and examples of how to utilize the Framework.**

Will this preliminary draft, as presented:

- *be inclusive of, and not disruptive to, effective privacy practices in use today, including widely used voluntary consensus standards that are not yet final;*

- *enable organizations to use the Privacy Framework in conjunction with the Framework for Improving Critical Infrastructure Cybersecurity to collaboratively address privacy and cybersecurity risks; and*
- enable organizations to adapt to privacy risks arising from emerging technologies such as the Internet *of Things and artificial intelligence?*
  - **Our reviewers noted the Framework is intentionally flexible to allow for expansion and changes as technology continues to evolve. We see no conflicts with existing standards.**

Respectfully submitted,

Vickie Classen
Chair, Professional Issues Committee

Key ALGA Contributors:
Vickie Classen, Colorado Springs, CO, Office of the City Auditor
Chris Constantin, City of Chico, CA, Office of the City Manager

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/ Editorial/ Technical)
1	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	18	617	Appendix A	The suggested approach to risk based creation of the current profile should encourage organizations to methodically define their existing practices.		General
2	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	5	181	1.1	Same as above		General
3	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	6	215 - 247	1.1	The description of problems for individuals was refreshingly simple and straightforward. Using problems as a generic means to convey the complex issues faced with privacy concerns should help organizations focus on impact to their users.		General
4	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	6	239	1.1	However the wording on line 239 related to “problematic data action”, seemed weak and may not provide enough context to explain how to assess impacts.	Consider adding to the explanation or providing some examples.	Editorial

5	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	1	All	Supplemental Materials	The Hypothetical Use Case Profiles in the Supplemental Materials were especially useful to improve understanding and use of the Privacy Framework, however links to these materials were only available through the web page for the Working Draft as related materials.	We suggest a link from Section 3.0 How to Use the Framework to these supplemental materials could improve understanding and adoption.	Editorial
6	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	33	All	All	Appendix D, along with the Privacy Risk Assessment Methodology (PRAM), provides a clear, useful methodology for assessing privacy risks.	Consider moving the entire Appendix D into the main document, or add more emphasis in the main document to encourage readers to look at the Appendix.	Editorial
7	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	6 & 19	202, 670		The diagrams on page 6 and page 19, combined with the color coding in Table 1 were good depictions of the interaction and difference between the two frameworks.		General
8	ALGA	Vickie Classen Victoria.Classen@ColoradoSprings.gov	10	306	2.1	Beginning with Section 2.1 The Core, the description of the Framework and its relationship between Functions, Categories, Sub categories, Current Profile and Target Profile was useful and comprehensive, however Table 2 of Appendix A, was easier to understand. The embedded links in table 2 to definitions were very helpful to the reader.	Consider adding in an embedded link in Section 2.1 to Appendix A to give readers direct access to a more thorough explanation and examples.	Editorial