November 13, 2015

Ellen D. Flint
Senior Assistant Attorney General
General Counsel Division, Business Transactions Section
Oregon Department of Justice
Salem, OR 97301

RE: State of Oregon's SaaS Template Terms and Conditions – Comments from ITAPS

Dear Ms. Flint:

Thank you for the opportunity to offer comments regarding Oregon's Draft Model Software as a Service (SaaS) Contract as circulated by Dianne Lancaster on October 14th. The Information Technology Alliance for Public Sector (ITAPS)[1] appreciates the State of Oregon's recognition that new and emerging technologies require a set of terms and conditions that are tailored to the technology service being acquired. You may recall that ITAPS raised concerns regarding Oregon's standard information technology services terms in a letter dated December 22, 2014 addressed to Assistant Attorney General Karen Johnson. In that letter, we pointed out that "cloud" or SaaS offerings require a separate template of terms and conditions. We therefore appreciate Oregon's willingness to develop a unique template of SaaS terms.

General Observations.
As a general statement, as is the practice in the industry, SaaS offerings and commercial cloud services are heavily discounted to be price competitive, and as such are standardized to support multi-client solutions. By definition, multi-tenant SaaS offerings are prebuilt solutions that are delivered in a consistent manner from the cloud to all subscribers.

Most SaaS vendors are not able from a practical perspective to contract with a client (whether a commercial or government customer) using unique contractual terms mandated by the client. The reason is because SaaS offerings, which rely on standardization across the client base for everything from code, to security to service levels, are very different from traditional software licenses and IT services projects. Accordingly, many of the contractual terms found in IT services or software license agreements do not apply. Applicable provisions will vary by provider and offering, but with very few exceptions, have to remain consistent across client subscribers in order for the SaaS provider to effectively deliver against the associated service and financial obligations.

[1] **About the IT Alliance for Public Sector (ITAPS).** ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more.

We believe that a model contract should serve as the starting point to be tailored to align with the selected service provider's offering. In this way, the State will be able to avail itself of the inherent benefits and savings that the SaaS offering provides.

As for Oregon's proposed template, we note that it is sixty (60) pages long, whereas the typical length of a base SaaS contract today is only a dozen pages or less. Our assessment of the draft template is that it maintains a considerable amount of language from what is best characterized as legacy, custom-developed software solutions. Provisions like hardware, hardware maintenance and support; work product ownership; project management; acceptance testing; pilot testing; listings of deliverables; time is of the essence; project plans; 15% holdback; transition services; and contractor's personnel are all things that might be in a custom developed software agreement, regardless of whether it is hosted on premise or not. These are not provisions that one would expect to find in a SaaS template.

In support of competitively priced standardized offerings, SaaS vendors have standard cloud services agreements and transaction documents that specify the terms and conditions under which their SaaS offerings are provided. Due to the multi-tenant delivery of the SaaS offerings, deviations from the practices, policies, and measures set out in the offering agreement for individual clients are generally not feasible. Just like when you put your valuables in a safe deposit box inside a bank's vault, you do not get to dictate the security for the bank or your special box. Additionally, certain elements of the indemnification, warranty and liability provisions in the draft template are well outside the norm for SaaS contracts. These elements, if not appropriately revised in the final template, will only serve to increase the cost of providing SaaS solutions to agency customers.

There are also a number of terms that we would expect to include in a final negotiated agreement that are specific to SaaS contracts. These terms include, without limitation, right of access to services, infrastructure and documentation, and support services. SaaS providers will also have standardized service level agreements against which performance of their solutions are measured.

Data Security.
The data center facilities of SaaS providers adhere to established operational and security policies and procedures. Practically speaking, it would not be feasible from an operational, compliance, audit, or financial perspective to customize the operational and security aspects of multi-tenant SaaS offerings to each client's specific requirements.

Often the SaaS provider will provide its clients with a data security and privacy principles document that is referenced in the agreement and describes overarching practices and policies designed to defend the SaaS offerings against such risks as accidental loss, unlawful intrusions, unauthorized access, and unauthorized use of client data.

Most IT vendors with SaaS offerings take a "black box approach" in that the government entity is buying a space; the SasS vendor doesn't have access nor does it want access to the data being stored. The SaaS vendor should not be responsible if a government agency stores highly sensitive information that it shouldn't be storing in a SaaS environment. We recognize that some types of SaaS offerings, such as HR or financial systems, are designed to house sensitive information. For those, Oregon will want more insight and knowledge of the security standards provided with the

offering. But in instances where the State is buying an off-the-shelf multi-tenant service, it cannot expect the SaaS provider to tailor its security to fit Oregon's specific requirements. Rather, Oregon should select a vendor that has a strong security program, and adopt those standards internally. Oregon can validate the vendor's security through third party referenced standards such as FedRAMP and NIST guidelines, as used by the federal government.

Audit.
Because commercial cloud services operate at the provider's direction and control, evidence of each solution's compliance with applicable standards and regulations is provided to the client in an independent third party audit summary report. Granting one client the right to directly access and audit a commercial cloud service may violate the rights of, and agreements with, other subscribers and their data subjects. Furthermore, allowing one client to directly access and audit a commercial cloud service may compromise the security and integrity of the service.

Ownership.
The client pays a non-refundable subscription fee, which entitles the client to access a prebuilt solution for the corresponding term (i.e., annually). The client does not acquire assets through the client's access and use of the SaaS offering, and therefore, transfer of assets at termination does not apply.

Comments on Specific Provisions.
Upon request, ITAPS can provide comments on various sections of Oregon's draft template, for your consideration.

In closing, we hope that our input provides the State of Oregon with insights on SaaS contracting, which will in turn enable the State to incorporate more "SaaS compatible" and commercially acceptable terms and conditions into its SaaS template and which would then be the basis of negotiations with the intended awardee. If not, we believe the result is likely to be fewer bidders (i.e. less competition), which almost always results in prices that are not the most competitive and which may not provide the State with the SaaS solution that best fits the State's requirements. Aligning Oregon's SaaS terms and conditions so that they converge with IT industry best practices will be advantageous to the State and its taxpayers.

Thank you for your attention to this matter.

Sincerely,

Carol Henton

Carol Henton
State, Local and Education Technology

cc: Dianne Lancaster, Chief Procurement Officer, Department of Administrative Services
Alex Pettit, Chief Information Officer (CIO)
Sean Vinck, Deputy Chief Information Officer