CENTER FOR DIGITAL GOVERNMENT

BEST PRACTICE GUIDE FOR

CLOUD AND AS-A-SERVICE PROCUREMENTS

digital communities

DIGITAL STATES PERFORMANCE INSTITUTE

EXECUTIVE SUMMARY

The delivery of information and communication technology (ICT) services is fundamentally changing. Internet- or cloud-based services are replacing traditional local — or on-premises — software and infrastructure installations for many state and local governments. While technology service options continue to evolve, however, procurement processes and policies have remained firmly rooted in historical practices that are no longer effective. In order for governments of all sizes to take advantage of the best the market now has to offer, a more flexible and agile procurement process must be identified and implemented. This guide, built upon the collaborative work of state and local government and industry executives, seeks to outline and explain what those changes might look like.

State and local governments must not isolate themselves from the change taking place in society and the technology market, but rather position themselves to embrace and benefit from it.

This guide started when the Center for Digital Government, through its Digital States Performance Institute and Digital Communities Program, joined with New Jersey CIO Steve Emanuel to invite a select group of public and private sector leaders to an inaugural meeting in January 2014 in Trenton, N.J. The purpose of that meeting was to determine if participants could come to an agreement on best practices for the timely and effective procurement of new services. Working initially from terms and conditions pioneered by Delaware to support its Cloud First Policy, the workgroup shared ideas and perspectives on terms and conditions related to Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), as defined by the National Institute of Standards and Technology (NIST).

Over the next five months, which included two more face-to-face meetings and dozens of conference calls, the workgroup identified a number of potential improvements to state and local government procurement policies. This guide chronicles that effort and those improvements. It is designed to serve as a reference document so it has been divided into multiple sections. Throughout the main body of the report, specific terms and conditions are grouped according to general function and purpose. Proposed language that could be included in procurement documents is provided for each of the following major categories:

- **Service Models**
- **Data**
- **Breach Notification**
- **Personnel**
- **Security**
- **Audits**
- **Operations**

These sections, together with the appendices, provide:

- Model terms and conditions language suitable for inclusion in procurement documents
- Guiding principles to be considered when evaluating "X-as-a-Service" (XaaS) solutions and offerings
- Recommendations for modernizing and improving procurement approaches
- Lessons learned from some early public sector adopters

This guide provides a backdrop and foundation for change, but change will not occur without purposeful action. If state

and local governments want to enjoy the benefits of XaaS, policy makers, finance directors, auditors, procurement officers, attorneys and, ultimately, elected officials, must reconsider and modernize the controls and processes that currently create barriers to accessing these services. The following recommendations will help these leaders get started on a path of change:

- Use the model terms and conditions in this report as a foundation to frame new service relationships.
- Make the changes necessary to modernize and improve procurement infrastructure and acquisition processes.
- Develop alternative controls to protect the public interest that enable the use of XaaS when it best meets the need.

State and local governments must not isolate themselves from the change taking place in society and the technology market, but rather position themselves to embrace and benefit from it. It is time to move confidently toward a new set of commercially proven practices that support innovation and collaboration through Internet-based services.

This guide has been a collaborative effort and contains the contributions and collective views of several authors representing various companies, governmental agencies or themselves. Each contributor is responsible for his/her own views and opinions which may or may not be expressed in this guide. Such opinions are not necessarily those of e.Republic or of any of the other contributors. This guide contains general information only and should not be considered as professional advice or services of any nature, and it is not intended as a substitute for any such advice or services.

INTRODUCTION

The Center for Digital Government, through its Digital States Performance Institute and Digital Communities Program, joined with New Jersey CIO Steve Emanuel to invite a select group of public and private sector leaders to an inaugural meeting in January 2014 in Trenton, N.J. The purpose of that meeting was to determine if participants could come to an agreement on best practices for the timely and effective procurement of new services. The workgroup shared ideas and perspectives on terms and conditions related to Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), as defined by the National Institute of Standards and Technology (NIST).

The language of technology procurement in government is rapidly and profoundly changing, and that has created confusion and uncertainty in the market.

Building on the work that began in New Jersey, two more face-to-face meetings and dozens of conference calls were convened over the next five months until the workgroup identified a number of potential improvements to state and local government procurement policies.

To understand the importance of this consensus among leaders, one must first understand the initial challenge. The language of technology procurement in government is rapidly and profoundly changing, and this has created confusion and uncertainty in the market. New business models for delivering IT services are becoming increasingly popular. "Anything-as-a-Service" or "X-as-a-Service" (XaaS) are two names for cloud-based services delivered to customers over the Internet. The most common service models used in government today are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), although other models such as Communication-as-a-Service (CaaS) and Monitoring-as-a-Service (MaaS) are now available. The two most common ways to pay for these types of services are to "pay as you go" or through a subscription model, which is radically different than the way traditional technology solutions are purchased. These emerging business models present challenges for traditional public procurement practices and the contracting relationships used by many state and local governments.

The initial question for the workgroup, raised at the inaugural meeting in New Jersey, was: Is it possible for public and private sector leaders to identify and share examples of what is working best, and then come to substantial agreement on key provisions that would lead to more timely and effective procurement of these new services? The group worked initially from terms and conditions (T&Cs) pioneered by Delaware CIO Jim Sills, CISO Elayne Starkey and Chief Procurement Officer Dean Stotler that were developed for the state's Cloud First Policy. Georgia CTO Steve Nichols provided the foundation work necessary to transition the Delaware examples to a broader audience by analyzing and comparing Delaware's T&Cs to Georgia's recent contracting experience.

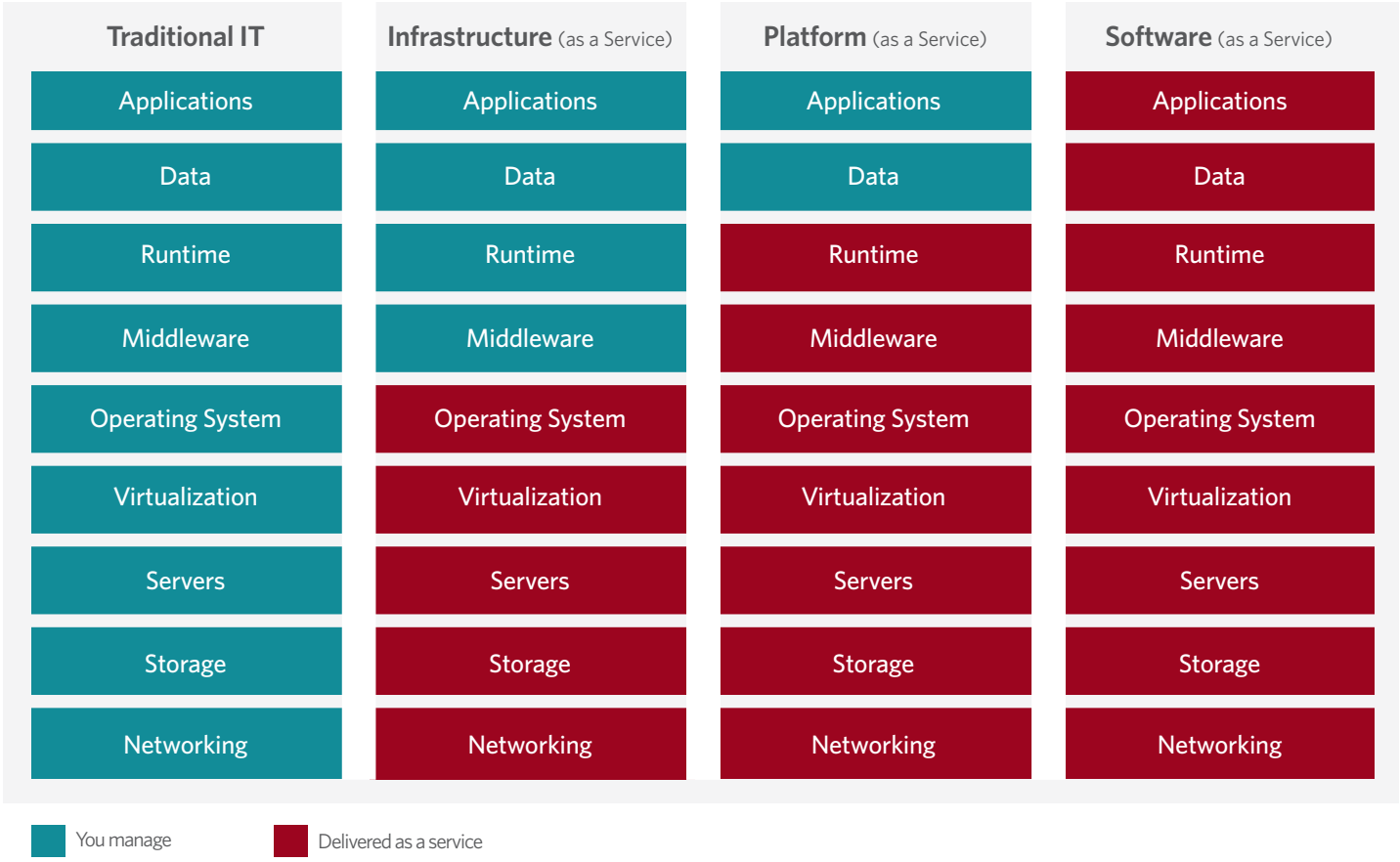
After a day of discussion, characterized by a broad range of diverse perspectives, the workgroup reached agreement on several key contract terms. Emanuel challenged the group by asking, "What actions can we take? What can we quickly put in place that will give our work value and create improvements for our states and the taxpayers?"

Over the next five months, the group addressed those questions by agreeing on T&Cs for SaaS, PaaS and IaaS models. The T&Cs templates developed by the workgroup offer state and local governments an excellent starting point for XaaS contracts, while recognizing that each procurement will likely have at least a few unique requirements that need to be further negotiated.

Along the way, through an open exchange of ideas, the group also came to a consensus on guiding principles that can help public jurisdictions and industry providers better approach and understand the relationships created by XaaS contracting, as well as help improve public procurement practices to achieve better outcomes while protecting the public interest.

In addition, the State of Texas, the Commonwealth of Massachusetts and other public jurisdictions shared their experiences and lessons learned as early adopters of XaaS procurements. This guide contains the answer to the question first raised in New Jersey and describes what can quickly be put into place that will create value and benefit for public jurisdictions and taxpayers.

Public Sector Management of XaaS Platforms



Source: Adapted from IDC Government Insights

SPECIFIC ISSUES AND THE PATH TO CONSENSUS

As workgroup members began to closely examine the specific T&Cs of the Delaware model, it quickly became clear that needs, expectations and desires of the participants were not consistent. During the discussion, a number of issues and perspectives emerged on data, security, breach notification, contract termination, legal notice and service provider operations. The following section provides background information on these issues and how the workgroup eventually addressed them with contract clauses for each service model. It provides insight into the concerns and perspectives of both service providers and public jurisdictions. Finally, it provides clarification useful to both government leaders and service providers as they approach and implement XaaS contracts.

Service Models

There was confusion in the first workgroup meeting because service providers and government participants viewed the terms from their unique perspective of a SaaS, PaaS, IaaS or hybrid service. Finding agreement on terms that worked for each service model proved to be difficult.

The workgroup began to make progress in the second meeting, when members discussed the terms and conditions from the perspective of a specific definition of each service model. The model T&Cs are intended to work with service models as defined by NIST (outlined in this section).[1] By looking at each term through the specific service model lens, the workgroup identified and resolved concerns regarding each model. This is a helpful lesson for public jurisdictions and service providers as they attempt to adopt the right T&Cs for their XaaS contract. A full understanding of the XaaS architecture and the party's respective responsibilities for control and operation of the stack of software and hardware is an essential first step to developing the appropriate T&Cs and service level agreements. While many of the terms are the same across the three service models, one size does not fit all.

Software-as-a-Service (SaaS) is "the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

In this model, as shown in Table 1, the service provider owns and operates all software and hardware needed to provide the service. Only limited controls are available to the public jurisdiction. The model is suited for full-service applications accessed by end users within an organization. It requires a minimal level of support by the jurisdiction. Applications range from email and collaboration tools to office productivity tools/suites to integrated ERP systems.

Platform-as-a-Service (PaaS) is "the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications using

Table 1: SaaS Technology Stack Controls[2]

Service Provider	Technology Stack	Public Jurisdiction
Administrative Control	Application (e.g., mail)	Limited Admin Control User Level Control
Total Control	Middleware (e.g., java)	No Control
Total Control	Operating System	No Control
Total Control	Hardware	No Control

programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations."

With this service model, the public jurisdiction has complete control over its application software and program control over middleware. The service is suited for public jurisdictions that want to use the PaaS provider's tools to develop, deploy and administer applications to its end-user customers.

Infrastructure-as-a-Service (IaaS) is "the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not

Table 2: PaaS Technology Stack Controls[3]

Service Provider	Technology Stack	Public Jurisdiction
No Control	Application (e.g., mail)	Admin Control
Admin Control	Middleware (e.g., java)	Program Control
Total Control	Operating System	No Control

manage or control the underlying cloud infrastructure, but has control over operating systems, storage and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."

The service provider maintains control over the hardware and administrative control over the hypervisor that uses the hardware to synthesize one or more virtual machines. The public jurisdiction maintains control over the operation of the guest operating system and all the software layers above it. In this model, the consumer may make requests to create and manage new virtual machines. The public jurisdiction assumes the greatest operational control responsibility. This model is suited to a public jurisdiction where systems administrators need quick access to virtual computing and storage capacity.

Different Terms and Conditions

The service models do not all work the same way. As a result, the three model T&Cs share many common clauses, but those dealing with operational responsibilities (e.g. data protection, security incident or breach notification, breach

Table 3: IaaS Technology Stack Controls[4]

Service Provider	Technology Stack	Public Jurisdiction
No Control	Application (e.g., mail)	Total Control
No Control	Middleware (e.g., java)	Total Control
No Control	Guest Operating System	Total Control
Administrative Control	Hypervisor	Make Requests
Total Control	Hardware	No Control

responsibilities, access to security logs and reports, and encryption of data at rest) vary. For example, a SaaS service provider is responsible for most of the technology stack and for these clauses. The service provider has more and broader responsibility for protecting data and reporting. However, the IaaS service provider is essentially leasing the infrastructure to the public jurisdiction, requiring the public jurisdiction to be responsible for its own data protection, encryption and reporting. Additionally, termination and suspension of service is managed differently for SaaS contracts than for PaaS and IaaS. SaaS contracts specifically require a service provider to maintain data for up to 10 days after a contract expires in accord with the termination timelines. Finally, clauses dealing with compliance for application accessibility standards and requiring Web services are simply not applicable to IaaS contracts.

Data

Ownership of Data

Governments have a fundamental responsibility to limit access to non-public information and to protect the integrity of their data. It is critical for a public jurisdiction and the service provider to affirm the jurisdiction's ownership of its data and how it is to be managed. This is typically a mandatory provision for public jurisdictions. Key public jurisdiction concerns that should be addressed in a data ownership clause include:

- Public jurisdictions must protect the privacy of certain citizen information. To protect privacy, the public jurisdiction must control and continuously own the data, including personally identifiable information (PII) and protected health information (PHI). Personal data is defined in **Clause 1 Definitions*** to cover both PII and PHI. Regardless of the type of service selected to process and manage the data, the public jurisdiction still has a duty as owner to comply with state and federal laws requiring protection of PII and PHI. Protection of data in a XaaS contract is often a shared responsibility. Specific roles and responsibilities should be clearly identified within the service level agreement (SLA).
- Data must not be accessed for any purposes except those authorized by the public jurisdiction. Establishing ownership and prohibiting the provider from accessing the data or user accounts for any purpose not authorized by the government limits access to the minimum level needed to perform the services of the contact. **Clause 2 Data Ownership** affirms data ownership, restricts access to the data to use within the provider's data center and then only for the intended purposes of the contract, and prevents access to the data for any other purpose except as authorized by the jurisdiction in writing.
- **Clause 3 Data Protection** requires the service provider to protect the confidentiality and integrity of a public jurisdiction's data. It requires the service provider to encrypt both personal data and non-public data. Non-public data is defined in **Clause 1 Definitions** to cover all data deemed sensitive by the jurisdiction that requires some level of protection. This is typically information that is exempt from public records requests. Providers are prohibited from using the data for any purpose not intended or authorized. This includes copying, disclosing or otherwise using the data or any information collected under the contact for purposes not required as part of the services under the contract or authorized by the government.

Governments have a fundamental responsibility to limit access to non-public information and to protect the integrity of their data.

- The treatment of data, including treatment of sensitive data, is a key cost factor for service providers. Unique data requirements create both constraints and costs. To manage costs and constraints, a thorough understanding of the data controlled and managed by the XaaS provider is essential for both the public jurisdiction and the service provider.

** Clauses can be found in Appendix 1.*

- Public jurisdictions can protect the security and integrity of data through encryption. Depending on the type of service received under the contract, identity access management and encryption could be a public jurisdiction responsibility, provider responsibility or a joint responsibility. The SLA must include a clear delineation of responsibilities based on the nature of the relationship. **Data Protection Clause 3** makes it the service provider's responsibility to encrypt and otherwise protect personal data and non-public data for SaaS. However, in an IaaS model, the public jurisdiction is responsible for encryption and protection of its data. It is critical that the public jurisdiction understand the integration of data architectures between its on-premises systems and those of the service providers', the roles and responsibilities for software and system control, and data flow. Each party may have responsibilities that cannot be performed by the other. These must be understood and identified in the SLA and contract. NIST provides an excellent reference framework in its Cloud Computing Architecture.

Location of Data

Public jurisdictions want services provided from and their data maintained in data centers located within the United States. Data and services provided outside the United States are subject to the laws of the country where the data is physically stored. By requiring services to be provided from data centers within the United States, public jurisdictions are certain about laws impacting their data. **Clause 4 Data Location** requires the service provider to:

- Provide services only from data centers located within the United States
- Prevent employees or subcontractors from storing public jurisdiction data on portable devices except as used in data centers within the United States
- Permits use of "Follow-the-Sun" technical support concept when needed for 24/7 end-user support

Import and Export of Data

Public cloud XaaS models are attractive to public jurisdictions in part because they allow rapid provisioning of applications using public jurisdictions' data. This may mean moving data and applications between service providers. As cloud-driven service models proliferate, it will be important for government agencies to be prepared for smooth disengagement and reengagement between service providers.

Clause 16 Import and Export of Data affirms the public jurisdiction's ability to import and/or export its data in whole or in part at the public jurisdiction's sole discretion with the cooperation of the service provider.

Breach Notification

Security Incident and Breach Notification

All public jurisdictions are critically concerned about protecting PII and other sensitive data. In the event of an incident, a public jurisdiction must take action both internally and through service providers to monitor and investigate. Of course, not all incidents result in a security breach. Prompt notice of an incident gives an agency more time to take any actions needed to address the incident. It also allows the agency to understand what appropriate actions the service provider is taking to protect personal data and non-public data.

Forty-seven states have laws that govern actions in the event of a security breach of personal information.[5] NIST defines PII as, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."[6]

A Congressional Research Service report described state security breach notification laws as generally following a similar framework and characterized by similar elements, including:

- Identifying who must comply with the law
- Defining the terms "personal information" and "breach of security"
- Establishing elements of harm that must occur, if any, for notice to be triggered
- Adopting requirements for notice
- Creating exemptions and safe harbors
- Clarifying preemptions and relationships to federal laws
- Creating penalties, enforcement authorities and remedies[7]

In addition to state laws covering PII, there are federal laws to protect health information. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), covered entities holding protected health information (PHI) must comply with privacy rules, including the HIPAA Breach Notification Rule, 45 CFR 164.400.

Security policies adopted by state and local governments guide the security of the technology systems they operate. These policies also guide compliance with state and federal laws. When entering into a contract with an XaaS provider, it is important to understand and apply the elements of the policy that are applicable to the service model that will be under contract. Not all policies will make sense or should be applied, but the requirements set by law must be addressed.

Service providers that have contracts with entities covered under HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) typically have security procedures in place to protect PII and PHI data. Their breach notification procedures must be designed to comply with these federal requirements.

To effectively protect personal data, the service provider and public jurisdiction must understand what constitutes

a breach. Contract terms must align with state laws to require service providers to detect data breaches and notify the public jurisdiction in a way that enables the public jurisdiction to comply with its obligations under law.

Prompt notice of an incident gives an agency more time to take any actions needed to address the incident. It also allows the agency to understand what appropriate actions the service provider is taking to protect personal data and non-public data.

Clause 5 Security Incident or Data Breach Notification requires a service provider to notify the public jurisdiction of a data breach. Data breach is defined in **Clause 1 Definitions** as the unauthorized access by non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data. Personal data is defined to include PII or PHI, but the clause allows for individual state definitions to take precedence over any other definition of PII. Data breach notification requires the service provider to notify the appropriate designated contact person by telephone within 24 hours of the time the service provider has actual knowledge of a confirmed data breach of personal data, unless applicable law requires a faster notification.

Non-public data typically does not have the same legal requirements for reporting as PII. A potential loss, theft or unauthorized access to unencrypted non-public data or personal data must be reported immediately as a security incident to the designated contact person. A public jurisdiction must clarify what is meant by "immediately" and outline other reporting requirements in the SLA.

Breach Responsibilities

Often one of the most difficult contract terms to define and agree on is the liability the service provider agrees to assume. It is very hard for either party in a contract to define the risk and the potential cost involved if there is a situation where the clause is triggered.

Service providers not only have a fiduciary duty to shareholders, but also have legal reporting requirements under Sarbanes-Oxley (SOX). Under section 302 of SOX, service provider management is required to have systems in place to identify material information that must be disclosed to investors and other third parties who rely on financial statements of publically traded companies.[8] This makes it difficult for a service provider to agree to unlimited liability in a contract of significant size. When a service provider cannot quantify its potential liabilities, it makes it very difficult to enter into an agreement.

The issue of unlimited liability has been addressed in more traditional IT contracts in some states by creating a liability cap calculated as a multiplier of the total contract value (i.e. 2X contract value). **Clause 6 Breach Responsibilities** uses a similar method to create a known amount for which the service provider is liable if the provider is the cause of a breach. The cap amount must be sufficient to cover all costs needed to address a breach.

It creates a definitive amount that is understood by both parties. This answers the service provider's question of what is the quantifiable exposure if a data breach occurs. It also answers the question of what the public jurisdiction will receive in the event of a breach. The approach seems to be a fair and reasonable way to apportion risk and mitigate damages in the event of a breach.

- The liability for a data breach caused by the service provider recommendation in **Clause 6 Breach Responsibilities** is based on studies conducted annually by the Ponemon Institute. In its most recent 2014 Cost of Data Breach study, the global average cost paid in 2013 for each lost or stolen record on a per-person basis in the United States was $201 per record.[9] The Ponemon samples do not specifically benchmark public sector data breaches in the United States, but they provide a place to start when seeking to quantify data breach mitigation costs.
- **Clause 6 Breach Responsibilities** requires the service provider to pay the cost of the breach investigation, resolution, notification, credit monitoring and call centers support up to a set amount per record/per person, if the service provider is responsible for the data breach. The service provider will take corrective action to mitigate the breach based on a root cause analysis.
- Finally, public jurisdictions must pay attention to the last sentence of **Clause 6 Breach Responsibilities**. It limits service providers' collective obligations and liabilities by limiting them to all corrective actions, "… as reasonably determined by service provider based on root cause … subject to this contract's limitation of liability."

Legal Requests

Public jurisdictions must be aware of legal requests that might require access to their data. As data owners, any request for access to the data should come to them. Most public information is available upon request, however, public jurisdictions are subject to specific state and local rules and laws governing the protection of the public's data that vary from place to place. If the public jurisdiction is a party to legal proceedings, any request for legal information must appropriately come to the public jurisdiction.

Clause 7 Notification of Legal Requests protects the public jurisdiction by requiring that the service provider contact the public jurisdiction when it receives a request for electronic discovery, a litigation hold, a discovery search or an expert witnesses request related specifically to public jurisdiction data stored by the service provider under the contract. It further restricts the service provider from responding to subpoenas, service of process and other legal requests without notifying the public jurisdiction, unless prohibited by law.

Termination and Suspension

Any service contract must be clear about how it can be terminated. With XaaS contracts, there is more to consider than just a cessation of services and accounting for final billings. With XaaS contracts, public jurisdictions must be sure they receive their data in an agreeable format that enables them to move the data to another provider or to their own on-premises solution.

- Depending on the nature of the service received and the circumstances under which the services are terminated,

there are timing concerns for the transfer of data. Providers want to dispose of data as quickly as possible since its continued storage is a cost to the service provider. A public jurisdiction will expect a service provider to securely dispose of data immediately after data is transferred to a new provider or the public jurisdiction's own on-premises solution. The contract terms and conditions need to reflect reasonable timelines, acceptable to both the jurisdiction and the provider, for the retention and disposal of the data.

- The amount of time the service provider must continue to store and make the data accessible to the jurisdiction largely depends on the circumstance of the termination. Contracts that reach their natural expiration point have a known termination date so the issue should not be a surprise to either party. In this case, the period that the provider must wait to dispose of the data is the shortest. Contracts that are terminated for convenience or for cause, however, come with less opportunity to plan and should provide public jurisdictions with a longer window prior to data disposal.
- Typically disposal should consist of destruction of all files and data in all forms, in accordance with NIST-approved standards, to prevent any further use or misuse of the information. The service provider should provide the public jurisdiction with appropriate certifications to document the disposal. Certifications protect both parties by documenting the method and date of destruction.
- Since a suspended service may be reinstated, an understanding of how the data will be preserved is important. If the service is reinstated, the data will be used. If the contract is not reinstated, it will be terminated and disposal of data would follow the prescribed steps specified under contract termination.
- **Clause 8 Termination and Suspension of Service** addresses these issues by requiring the service provider to return all public jurisdiction data in an orderly and agreed upon format. The specific service model can make a difference in the data transfer and disposal protocols. As a result, the specific time periods are different for the SaaS clause than for the PaaS and IaaS clauses. Each clause sets out specific time periods in which the service provider must continue to maintain the data. The service provider agrees to provide any post-termination assistance that it generally makes available to other clients, unless the parties agree to a specific and unique procedure in the SLA. The service provider agrees to destroy all data when requested by the public jurisdiction in accordance with NIST-approved methods and provide a certificate of destruction.

Personnel

Background Checks of Personnel

One of the biggest threats to data security can be internal. Public jurisdictions have a duty to protect their data no matter where it is and who is handling it. A prudent practice in contracting for services is to make sure the service provider's team has a background that is free of dishonesty, fraud or other offenses that could jeopardize the security of data.

Clause 9 Background Checks requires the service provider to conduct criminal background checks on its employees and subcontractors. Service providers are prevented from utilizing staff that fail the background check. The clause further makes it a duty of the service provider to promote and maintain the awareness and importance of securing the public jurisdiction's information.

Separation of Duties and Non-Disclosure

One way that public jurisdictions help protect their data and information is to limit the number of staff with access to their data. With sensitive and PII data, reducing the exposure of the information to others reduces the risk of breach and loss of privacy. Service providers with a wide variety of clients are sensitive to this concern and typically have procedures in place to limit the knowledge of customer data to essential staff, as well as require staff to sign non-disclosure agreements.

Clause 15 Non-Disclosure and Separation of Duties requires the service provider to enforce separation of job duties and limit staff knowledge of customer data to staff that absolutely need the knowledge to perform their job duties. Commercially reasonable non-disclosure agreements are required of the service provider for their staff handling this data.

A prudent practice in contracting for services is to make sure the service provider's team has a background that is free of dishonesty, fraud or other offenses that could jeopardize the security of data.

Right to Remove Personnel

An effective working relationship between the service provider and the public jurisdiction is critical to the success of a service relationship. The public jurisdiction can ensure the working relationship remains positive and productive by maintaining the right to require the service provider to remove any service provider representative who is detrimental to that relationship. This ability can also provide recourse to the public jurisdiction when a service provider representative compromises the security of the jurisdiction's data.

Clause 19 Right to Remove Individuals establishes the right of public jurisdictions to require the removal of service provider representatives and sets out conditions for their removal. A representative can be staff or subcontractor personnel. In the event of a potential security violation, the removal must be immediate.

Security

A public jurisdiction is obligated to protect the integrity and security of the public's data. To uphold the public's trust, a public jurisdiction entering into XaaS contracts must perform due diligence on the service provider, including determining whether the service provider has sufficient and adequate security processes in place to protect and safeguard the data.

SaaS solutions are wide ranging in their applications and in some cases their use of second-tier subcontractors. A thorough review and assessment of security procedures provides good protection for a public jurisdiction. If internal security resources are limited, jurisdictions can engage a qualified third party to perform an assessment.

Any assessment should include a review of the service provider's technical security procedures to ensure security is commensurate with the level of data classification to be stored and managed by the provider. To obtain a full and complete assessment of the security chain, both the service provider and the jurisdiction must understand their respective roles and responsibility for data security. A framework for assessment can be found in ISO 27001. Although not a requirement, FedRAMP-certified service providers can make the due diligence of security assessments much easier. Another third-party security report from the service provider that includes independently audited AICPA Service Organization Control (SOC) 2 report can also support security due diligence requirements.

Clause 14 Security requires the service provider to disclose its non-proprietary security process and any technical limitations. It requires a joint understanding of respective roles and responsibilities by each party.

Security Logs and Reports

Security officers in public jurisdictions use security logs when investigating an incident to determine if data has been lost or compromised. For a public cloud service provider, sharing technical information such as security logs creates vulnerabilities for the provider. Service providers believe their unique reports would be difficult for public jurisdictions to decipher in any meaningful way. To address this issue, service providers typically are willing to pledge their cooperation to assist a customer in the event of an incident. Service providers also often provide summaries and other reports that provide the information a customer may need.

Public jurisdictions need meaningful and relevant reports, statistics, access information and security log information to understand vulnerabilities and threats to their data and systems when linked to the service provider. Service providers must share access information with their clients to assist them in assessing their vulnerabilities and responding to threats and attacks. At the same time, service providers have a duty to all their clients to not disclose information that creates vulnerabilities. From a business model perspective, the service provider cannot create expensive and unique services that aren't included in the SLA, or in the case of public cloud offerings, consistent with the general

service offering. Clear expectations and responsibilities must be spelled out and agreed to in the SLA.

Clause 10 Access to Security Logs and Reports requires the service provider to provide reports that include latency statistics, user access IP addresses, user access history and security logs for the data covered under the contract. The clause requires the format for the reports to be specified to and agreed upon by both parties in the SLA.

Encryption of Data at Rest (Mobile Devices)

Some of the most notorious public data breaches involve data at rest. Data at rest typically refers to any data that is not transiting through a network via email, wireless transmission or other electronic interchange. It is data that resides in a database, file system, hard drive, portable storage device, memory or any other structured storage method. Data at rest, particularly in mobile devices (flash drives, laptops, tablets, etc.), is highly vulnerable to theft or loss. Data at rest in file servers and other structured data management systems is also at risk of attack.

Jurisdictions that classify their information and data can select the appropriate level of protection based on that data classification. Data that contains PII is critical to protect and typically has the highest data classification level. Public data is at the lower end of the classification scale. It is available to the public upon request and is often readily available on the public jurisdiction's portal. Since it has the lowest level of classification, it may not require special security treatment. Non-public data is sensitive information that is typically classified in the middle.

The primary security controls for restricting access to sensitive data such as PII and non-public data stored on end-user devices are encryption and authentication.[10] The specific level of protection or strength of encryption depends on the sensitivity of the data and the classification level set by the public jurisdiction. Service providers typically encrypt data in transit and at rest within their network. It is important that the jurisdiction understands the level of encryption required and affirms that it is the appropriate level for the classification of its data.

Data at rest, particularly in mobile devices (flash drives, laptops, tablets, etc.), is highly vulnerable to theft or loss. Data at rest in file servers and other structured data management systems is also at risk of attack.

Clause 23 Encryption of Data at Rest requires the service provider to prevent its employees and subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.[11]

Audits

The services delivered to the public through contracts require appropriate management and oversight to ensure the public's interests are served. In addition to the normal oversight and contract management, a variety of audit controls are used so independent parties can confirm the public's interests are protected. With XaaS-based service contracts, audits typically cover the following key areas:

- **Contract Compliance** — Is the public jurisdiction getting what is required by the contract? This is usually limited to determining if the parties to a contract are meeting their obligations under the contract and identifying any gaps in the performance of the contract. Contracts with clear performance expectations simplify audits.
- **Financial** — Are the payments consistent with the terms of the contract? When the contracted service supports financial reporting, the audits may examine the integrity of the information and data upon which reports depend.
- **Security** — Are appropriate security measures and protections in place to protect the data from unauthorized access and to keep it private and confidential?

Cloud service models are causing a major shift in how public jurisdictions set controls to protect the public's interest. Effective integration of XaaS-based contracts should start with a clear understanding of the public jurisdiction's business objectives and performance expectations. Next, the jurisdiction should examine its existing controls and their effectiveness in the "as is" process. The jurisdiction will then be in a position to decide what controls are needed to reasonably achieve its business objectives using a cloud-based service delivery model. A jurisdiction can also decide if existing controls will be effective, need to be adapted or if other control methods must be developed.

Audits are often viewed as a safeguard that permits independent parties to determine if service providers and public jurisdictions are meeting contractual requirements. Early detection of risks can help shore up a contract and put it back on track, but are not a substitute for good planning and contract management. Unclear or ambiguous business needs on the part of the public jurisdiction can create a risk of contract failure. Public jurisdictions can reduce their reliance on audits with a clear and in-depth understanding of their business needs and by conducting a thorough assessment of the service provider's capability to meet those needs. Emphasis should be placed on:

- Understanding internal business objectives
- Determining the performance required to meet those objectives
- Performing due diligence of the service provider's capabilities
- Relying on existing third-party certifications and compliance

A rapidly expanding range of proven service models that offer great opportunities and benefits are available to state and local governments.[12] Service providers can offer their catalog of services at a value point for their customers due to a high degree of standardization and the benefits of taking their business model to scale. Cloud service providers have described it as "one line of code for many." However, service cannot be delivered at a value point if

each customer expects a unique service, including unique and undefined potential audit obligations. Service providers typically seek to limit unique audits and rely on third-party audit reports and certifications of compliance with national standards.[13] The contract should be specific about the type of audit that will be performed, the frequency of the audit and the public jurisdiction's access to the audit.

Audits are often viewed as a safeguard that permits independent parties to determine if service providers and public jurisdictions are meeting contractual requirements. Early detection of risks can help shore up a contract and put it back on track, but are not a substitute for good planning and contract management.

State and local governments have an opportunity to improve government service delivery through responsible development of XaaS contracts. However, traditional control models — designed to protect and safeguard the public's interest — may prevent some public jurisdictions from taking advantage of new service models. Other policy makers in government, beyond procurement officials and CIOs, must look at their policies to identify barriers to the adoption of these service models. Appropriate oversight and control is a critical part of any public expenditure, but both must also be tailored to work effectively with the service model. Without this alignment, the full benefit or the service will not be received.

Clause 11 Contract Audit requires the service provider to audit conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction.

Clause 12 Data Center Audit requires the service provider to perform an independent audit annually for all of their data centers at the service provider's expense. A redacted version of the audit must be made available to the public jurisdiction if requested. The example sets an expectation of a SOC 2 or similar audit.

Operations

Operations Responsibility and Uptime Guarantee

System performance and service reliability are important to the business of public jurisdictions. CIOs know how little tolerance end users have for service outages — no matter the cause. Establishing clear service expectations in the terms and conditions is essential for XaaS contracting. Jurisdictions find it helpful to conduct market research before the procurement to know what to expect in the market and to make sure applications selected for XaaS contracts are well suited to expected operational reliability.

The nature of new cloud-based business models results in service providers relying on a variety of partners, subcontractors or other third parties to provide services to its customers.

The service provider and the public jurisdiction must agree to the specific details of service performance measure and maintenance downtime schedules in the SLA.

Clause 17 Responsibilities and Uptime Guarantee make the service provider responsible for all of the plant, capacity, hardware, software and personnel needed to provide the service, and commits the service provider to service 24/7.

Changes and Maintenance

Today's XaaS providers are providing performance through a service. Unlike traditional on-premises solutions that require upgrades and service maintenance contracts that expire, XaaS providers simply provide the service. For these business models to achieve economies of scale, the providers must use a "one line code" for all. Upgrades and changes are rolled out to all, not to individual users.

Even though the service is more seamless than on-premises systems of the past, public jurisdictions still need to keep their users apprised of any changes that could impact the performance of the system and their use of the services.

Clause 13 Change Control and Advance Notice requires the service provider to give advanced notice of upgrades or system changes that may impact the public jurisdiction's performance.

Subcontractors

The nature of new cloud-based business models results in service providers relying on a variety of partners, subcontractors or other third parties to provide services to its customers. For a public jurisdiction, it is important to identify the prime contractor and the various third-party providers and their relationship with the service provider. Ideally, a public jurisdiction will seek this information as a part of its pre-contracting due diligence.

Clause 18 Subcontractor Disclosure requires the service provider to identify all strategic business partners, subcontractors, and other entities and individuals who will be involved with the public jurisdiction's applications and data in the performance of the contract.

Operations Business Continuity and Disaster Recovery

For any application that supports business operations and business continuity, disaster recovery plans are critical to address potential public jurisdiction business disruptions and how the elements of the business will be returned to service. For any public jurisdiction XaaS business application, the contract recovery objectives should be aligned with the public jurisdiction's overall business continuity plan.

Clause 20 Business Continuity and Disaster Recovery requires a business continuity plan and a disaster recovery plan for the service provider's operations. It specifically requires the service provider to recover the public jurisdiction's data to meet recovery time objectives agreed upon by both parties. The details of the recovery time must be negotiated between the service provider and the public jurisdiction, and should be specific in the terms and conditions and SLA.

CONCLUSION

Many governments still try to buy XaaS through traditional procurement methods and standard contract terms and conditions, even though what they are buying is fundamentally different from traditional IT. This approach is not working.

Procurement processes that require strict conformance to prescribed specifications and unique terms and conditions are ineffective in the current technological environment. They were originally developed to acquire products, not services. Effective procurement achieves timely results and good outcomes, and protects the public's interest. That is all still possible through a more flexible, services-centric approach. Continued over-reliance on traditional state and local procurement policies, rules or statutes impedes effective procurement of technology services and unnecessarily inflates both a project's cost and delivery schedule.

The XaaS model of today relies on standardization and consistency in code, process, security and, ultimately, a business model supporting the delivery of service over the Internet. XaaS delivers value and benefit for its users because services are not unique to each purchaser. This creates tremendous efficiency and economy of scale. It may, however, require significant changes in government business practices.

If state and local governments want to take advantage of this service model, policy makers — finance directors, auditors, procurement officers, attorneys and elected officials — must reconsider and modernize their controls and processes that now create barriers to accessing these services. New ways to provide transparency and accountability must be identified and used that not only protect the public interest, but also enable the purchase of XaaS technology when appropriate.

New Jersey CIO Steve Emanuel asked, "What actions can we take? What things can we quickly put in place that will give our work value and create benefit for our states and the taxpayers?" The answers include:

- Use the model terms and conditions to frame these new service relationships
- Make the changes necessary to modernize and improve the procurement infrastructure and acquisition processes
- Develop alternative controls that protect the public interest and allow the use of XaaS when it best meets the need

The rapid proliferation of these service offerings is profoundly changing how the world does business. State and local governments must not isolate themselves from that change, but rather position themselves to embrace and benefit from it. It is the time to set aside outdated practices that inhibit progress, and move confidently toward a new set of commercially proven practices and procedures that support innovation, collaboration and economy through Internet-based services.

WORKGROUP MEMBERS AND CONTRIBUTORS

Workgroup Members

Sherry Amos, Managing Director, Industry Strategy, Education and Government Markets, Workday

Jason Barlow, Corporate Counsel for Public Sector and Commercial Law, Salesforce.com

Tonia Beam, Georgia Technology Authority, State of Georgia

Phil Bertolini, Deputy County Executive and Chief Information Officer, Oakland County, Michigan

Kurt Bittner, Account Manager, Panasonic Solutions for Business

Brad Booth, Account Manager, McAfee

Caralyn Brace, Vice President & General Manager North America, Technology, Consulting and Integration Solutions, Unisys Corporation

Gloria Broeker, Chief Operating Officer, Office of Information Technology, State of New Jersey

David Brown, General Counsel, Department of Information Resources, State of Texas

Michael DeAngelo, Deputy Chief Information Officer, State of Washington

Gregory DiFranco, Quality & Risk Management, Deloitte Consulting LLP

Stephen Elkins, Chief Information Officer, City of Austin, Texas

Steve Emanuel, Chief Technology / Information Officer, Office of Information Technology, State of New Jersey

Tony Encinias, Chief Information Officer, Commonwealth of Pennsylvania

John Essner, Chief Information Security Officer, Office of Information Technology, State of New Jersey

Wanda Gibson, Chief Technology Officer, Fairfax County, Virginia

Janet Gilmore, Director of Digital Government, Department of Information Resources, State of Texas

Tony Gomez, Director of Sales, AirWatch

Jim Harper, Regional Vice President, State and Local East, Salesforce.com

Bruce Hermes, Deputy Chief Information Officer, City of Austin, Texas

Bruce High, Chief Information Officer, Harris County, Texas

Ryan Hughes, Cloud Services Executive, Unisys Corporation

Todd Kimbriel, Chief Operations Officer, Department of Information Resources, State of Texas

Jane Lacy, Contracts Business Manager, World Wide Public Sector Government and Education Business Development, Amazon Web Services

Chad Lersch, Assistant General Counsel, Department of Information Resources, State of Texas

Denise Lucas, Deputy Purchasing Officer, City of Austin, Texas

Peni MacMeekin, Technology Licensing Officer, Division of Purchase and Property, Dept. of the Treasury, State of New Jersey

Joseph Mastrogiorgio, Vice President Sales, Cloud & IT Solutions Government and Education, East Region, Verizon-Terremark

Ryan Melody, Cloud Services, General Dynamics Information Technology

Contributors

Karen Miller, Supply Chain Manager, General Dynamics Information Technology

Kevin Moore, Assistant Director, Purchasing, New Jersey Department of Treasury

Sam Morton, Partner Business Manager, VMware

Edward Naybor, Vice President Sales, General Dynamics Information Technology

Steve Nichols, Chief Technology Officer, Georgia Technology Authority

Bill Oates, Chief Information Officer, Commonwealth of Massachusetts

Teri Pennington, Deputy Chief Information Officer for Operations and Communications and Technology, City of Austin, Texas

Rachel Pizarro, Principal, Enterprise Sales, Amazon Web Services

Karen Robinson, State Chief Information Officer and Executive Director for the Department of Information Resources, State of Texas

Kristin Russell, Director, Deloitte Digital

Teresa Shuchart, Deputy Chief Information Officer, Commonwealth of Pennsylvania

Craig Shinn, Executive Director, NIC, Texas.gov

Ann Shook, Director of SLG Business Development, EMC

James Sills, Chief Information Officer and Secretary of the Department of Technology and Information, State of Delaware

Kelly Silverstein, Administrative Analyst, Office of Information Technology, State of New Jersey

Mark Slafka, Capture Manager, U.S. Public Sector Sales, VMware

Kathleen Smith, Director of PMO, Office of Information Technology, State of New Jersey

Frank Snyder, Director of Sales, State & Local Government, Education, Dell Software

Elayne Starkey, Chief Security Officer, Department of Technology and Information, State of Delaware

Dean Stotler, Director of Government Support Services, State of Delaware, President of National Association of State Procurement Officers

Dawn Swainston, Director of Business Development, Symantec

Robert Woolley, Chief Technology Architect, Department of Technology Services, State of Utah

Shannon Kelley, Contract Manager, Enterprise Contract Management, Technology Sourcing Office, Texas Department of Information Resources

Gary Lambert, Assistant Secretary for Operational Services, Commonwealth of Massachusetts

Andrew P. Sidamon-Eristoff, State Treasurer, State of New Jersey

Dugan Petty, Senior Fellow, Center for Digital Government

Todd Sander, Executive Director, Center for Digital Government

Underwritten By

AirWatch by VMware is the leader in enterprise mobility management, with more than 12,000 global customers. The AirWatch platform includes industry-leading mobile device, email, application, content, and browser management solutions. Organizations can implement these solutions across device types and use cases, including complete EMM for corporate and line of business deployments, and containerized solutions for Bring Your Own Device (BYOD) programs. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at **www.air-watch.com.** VMware is headquartered in Silicon Valley and can be found online at **www.vmware.com.**

Amazon Web Services' Worldwide Public Sector Team offers enterprise class cloud computing services to Government, Education, Healthcare and Nonprofit organizations globally. With the cloud, public sector IT professionals no longer need to plan for IT infrastructure months in advance, but rather can be operational in minutes. Learn more at **http://aws.amazon.com/government-education.**

Dell empowers countries, communities, customers and people everywhere to use technology to realize their dreams. Dell delivers technology solutions that help customers do and achieve more, whether they're at home, work or school. Dell offers products, solutions and services that work "better together" to meet customers' needs. Dell Enterprise Solutions help customers realize an optimized enterprise. Dell Client Solutions provide customers and consumers with a complete range of highly reliable, secure, and manageable solutions. Dell Software makes it easy to secure and manage networks, systems, applications, endpoints, devices and data. Dell Services and Dell SecureWorks comprise more than 42,000 professionals in 90 countries. For more information, visit **www.dell.com.**

State government works best when empowered with the tools to serve its people. At **Deloitte**, our public sector experience and private sector insights shape understanding and deliver the answers you need to move forward in technology, financial management, workforce, operations, and more. As the world's largest consulting firm, we can help you take decisive action and achieve sustainable results. Learn more at **www.deloitte.com/us/stategovernment** and follow us at **@DeloitteGov.**

EMC Corporation is a global leader in enabling public sector agencies and institutions to transform their operations and deliver IT as a Service. Fundamental to the transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect, and analyze their most valuable asset — information — in a more agile, trusted, and cost-efficient way.

General Dynamics Information Technology serves as a leader in cloud computing, virtualization and data center transformation for government and commercial customers, developing robust IT Solutions to include:

- Data center transformation
- Private cloud implementation
- Cloud brokerage
- Unified communications and collaboration
- Virtual Desktop Infrastructure (VDI)
- Cyber security and identity management
- Next Generation 9-1-1

General Dynamics IT creates open architecture solutions that easily adapt to evolving software, hardware, data, services and management requirements while providing enhanced enterprise visibility and data security. The full-spectrum of services from design and development to integration, operations and maintenance, creates a true one-stop-shop to provide the service levels our customers demand.

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe.
www.mcafee.com

NIC is the nation's leading provider of official eGovernment services, mobile applications, websites, and secure payment processing solutions. The company's innovative eGovernment solutions use technology to help make government more accessible to everyone. NIC provides eGovernment services for more than 3,500 federal, state, and local agencies in the United States.
www.egov.com

Salesforce.com is the enterprise cloud computing leader dedicated to helping companies and government agencies transform into connected organizations through social and mobile technologies to connect with their customers, citizens, partners, and employees in entirely new ways. Since launching its first service in 2000, salesforce.com's list of 120,000+ customers spans multiple industries worldwide. The company's trusted cloud platform and apps are transforming 500 government agencies including the majority of the states and federal cabinet agencies that are using solutions for a multitude of functions from CRM, and call center management, to IT service management, social media monitoring, and others.

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Unisys is a global information technology company that solves complex IT challenges at the intersection of modern and mission critical.

We work with many of the world's largest companies and government organizations to secure and keep their mission critical operations running at peak performance; streamline and transform their data centers; enhance support to their end users and constituents; and modernize their enterprise applications. We do this while protecting and building on their legacy IT investments.

Our offerings include outsourcing and managed services, systems integration and consulting services, high-end server technology, cybersecurity and cloud management software, and maintenance and support services. Unisys has more than 23,000 employees serving clients around the world.

Verizon Public Sector (Verizon Connected Government) is the catalyst that drives success for agencies across federal, state and local government, as well as K-12, higher education, and public safety. Verizon Public Sector delivers an unparalled portfolio of cloud, mobility and security solutions over leading IP and 4G LTE networking platforms, offering flexibility, scalability and inherent security to meet the unique requirements of any government agency in the U.S. and abroad. Verizon investments enable public sector IT transformation programs by delivering tangible value, integrated security, and consistent and proven performance.
www.verizonenterprise.com/industry/public_sector/

VMware is the leader in virtualization and cloud infrastructure solutions that enable governments to thrive in the Cloud Era. More than 500,000 customers rely on VMware to transform the way they build, deliver and consume IT in a manner that is evolutionary and based on their specific needs.

Workday is a leading provider of enterprise cloud applications for human resources and finance. Founded in 2005, Workday delivers human capital management, financial management, and analytics applications designed for the world's largest organizations. Hundreds of organizations, ranging from medium-sized businesses to Fortune 50 enterprises, as well as education and government institutions, have selected Workday.

APPENDIX 1

Model Terms and Conditions Templates

The workgroup offers three templates as model terms and conditions for each specific service model: SaaS, PaaS and IaaS. As a model, each template is intended to accelerate the XaaS adoption by providing either a foundation or starting point for a public jurisdiction and a service provider to create a responsive and effective XaaS contract. As with any model document, the templates have no force or effect until used or adopted.

Software-as-a-Service

1. Definitions:

a. **"Authorized Persons"** means the service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **"Data Breach"** means the unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

c. **"Individually Identifiable Health Information"** means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[14]

d. **"Non-Public Data"** means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

e. **"Personal Data"** means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.

f. **"Protected Health Information" (PHI)** means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by

the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[15]

g. **"Public Jurisdiction"** means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

h. **"Public Jurisdiction Data"** means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

i. **"Public Jurisdiction Identified Contact"** means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

j. **"Security Incident"** means the potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

k. **"Service Level Agreement"** (SLA) means a written agreement between both the public jurisdiction and the service provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

l. **"Service Provider"** means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

m. **"Software-as-a-Service" (SaaS)** means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[16]

n. **"Statement of Work"** means a written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
b. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
c. All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of this contract.
d. Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit. The public jurisdiction shall identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
e. At no time shall any data or processes — that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
f. The service provider shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

4. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the

U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

5. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

a. **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.
b. **Security Incident Reporting Requirements:** The service provider shall report a security incident to the appropriate public jurisdiction identified contact immediately as defined in the SLA.
c. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

6. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
b. The service provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract

obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute[17] at the time of the data breach; and (5) complete all corrective actions as reasonably determined by service provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

7. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

8. Termination and Suspension of Service:

a. In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data in a CSV or another mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of public jurisdiction data.
b. During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
c. In the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
   - 10 days after the effective date of termination, if the termination is in accordance with the contract period
   - 30 days after the effective date of termination, if the termination is for convenience
   - 60 days after the effective date of termination, if the termination is for cause

   After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.
d. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the SLA.
e. The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National

Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

9. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA agreed to by both the service provider and the public jurisdiction. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this contract.

11. Contract Audit: The service provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense.

12. Data Center Audit: The service provider shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

13. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

14. Security: The service provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. For example: virus checking and port sniffing — the public jurisdiction and the service provider shall understand each other's roles and responsibilities.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

17. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

18. Subcontractor Disclosure: The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use Web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data, unless the public jurisdiction approves the storage of personal data on a service provider portable device in order to accomplish work as defined in the statement of work.

Platform-as-a-Service

1. Definitions:

a. **"Authorized Persons"** means the service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **"Data Breach"** means the unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

c. **"Individually Identifiable Health Information"** means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[18]

d. **"Non-Public Data"** means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

e. **"Personal Data"** means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.

f. **"Platform-as-a-Service" (PaaS)** means the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.[19]

g. **"Protected Health Information" (PHI)** means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by

the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[20]

h. **"Public Jurisdiction"** means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

i. **"Public Jurisdiction Data"** means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

j. **"Public Jurisdiction Identified Contact"** means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

k. **"Security Incident"** means the potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

l. **"Service Level Agreement" (SLA)** means a written agreement between the public jurisdiction and the service provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

m. **"Service Provider"** means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

n. **"Statement of Work"** means a written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions:

a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
b. All data obtained by the service provider within its control in the performance of this contract shall become and remain the property of the public jurisdiction.
c. Unless otherwise stipulated, personal data and non-public data shall be encrypted at rest and in transit with controlled access. The service level agreement (SLA) and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.
d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
e. At no time shall any data or processes — which either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

4. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

5. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach within the possession and control of the service provider and related to service provided under this contract.

a. **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law

enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed, defined by law or contained in the contract.

b. **Security Incident Reporting Requirements:** Unless otherwise stipulated, the service provider shall immediately report a security incident related to its service under the contract to the appropriate public jurisdiction identified contact as defined in the SLA.
c. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

6. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider and related to the service provided under this contract.

a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
b. The service provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law; all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute[21] at the time of the data breach; and (v) complete all corrective actions

as reasonably determined by service provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

7. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

8. Termination and Suspension of Service:

a. In the event of an early termination of the contract, the service provider shall allow for the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.
b. During any period of suspension, the service provider shall not take any action to intentionally erase any public jurisdiction digital content.
c. In the event of early termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of: 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of termination for cause, the service provider will impose no fees for access and retrieval of digital content to the customer.
d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all of its forms, such as disk, CD/DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

9. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

10. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA and agreed to by both the service provider and the public

jurisdiction. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this contract.

b. The service provider and the public jurisdiction recognize that security responsibilities are shared. The service provider is responsible for providing a secure infrastructure. The public jurisdiction is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

11. Contract Audit: The service provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense.

12. Data Center Audit: The service provider shall perform an independent audit of its data centers at least annually and at its own expense, and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

13. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

14. Security: The service provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. For example: virus checking and port sniffing – the public jurisdiction and the service provider shall understand each other's roles and responsibilities.

15. Non-Disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

17. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment is the responsibility of the service provider.

The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

18. Sub-Contractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who will be involved in any application development and/or operations.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) of XXX hours/ days is met. (XXX shall be negotiated by both parties.)

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use Web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Sensitive personal data, unless the service provider presents a justifiable position approved by the public jurisdiction that sensitive personal data must be stored on a service provider portable device in order to accomplish work as defined in the scope of work.

Infrastructure-as-a-Service

1. Definitions:

a. **"Authorized Persons"** means the service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **"Data Breach"** means the unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

c. **"Individually Identifiable Health Information"** means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[22]

d. **"Infrastructure-as-a-Service" (IaaS)** means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).

e. **"Non-Public Data"** means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

f. **"Personal Data"** means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.

g. **"Protected Health Information" (PHI)** means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA),

as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[23]

h. **"Public Jurisdiction"** means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

i. **"Public Jurisdiction Data"** means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

j. **"Public Jurisdiction Identified Contact"** means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

k. **"Security Incident"** means the potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

l. **"Service Level Agreement" (SLA)** means a written agreement between both the public jurisdiction and the service provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

m. **"Service Provider"** means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

n. **"Statement of Work"** means a written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service

provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions:

a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
b. All data obtained by the service provider within its control in the performance of this contract shall become and remain the property of the public jurisdiction.
c. Unless otherwise stipulated, personal data and non-public data shall be encrypted at rest and in transit with controlled access. The SLA and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.
d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
e. At no time shall any data or processes — which either belong to or are intended for the use of public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

4. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

5. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach related to public jurisdiction data within the possession or control of the service provider and related to the service provided under this contract.

a. **Security Incident Reporting Requirements:** Unless otherwise stipulated, the service provider shall immediately report a security incident related to its service under the contract to the appropriate public jurisdiction identified contact as defined in the SLA.
b. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that

affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

6. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of a service provider and related to service provided under this contract.

c. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

d. The service provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law; all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute[24] at the time of the data breach; and (5) complete all corrective actions as reasonably determined by the service provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

7. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

8. Termination and Suspension of Service:

a. In the event of an early termination of the contract, the service provider shall allow for the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.
b. During any period of suspension, the service provider shall not take any action to intentionally erase any public jurisdiction digital content.
c. In the event of early termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the service provider will impose no fees for access and retrieval of digital content to the customer.
d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all of its forms, such as disk, CD/DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

9. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

10. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction directly related to the infrastructure the service provider controls upon which the public jurisdiction account resides. Unless otherwise agreed to in the SLA, the service provider shall provide the public jurisdiction a history or all API calls for the public jurisdiction account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the service provider. The report will be sufficient to enable the public jurisdiction to perform security analysis, resource change tracking and compliance auditing.
b. The service provider and the public jurisdiction recognize that security responsibilities are shared. The service provider is responsible for providing a secure infrastructure. The public jurisdiction is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

11. Contract Audit: The service provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense.

12: Data Center Audit: The service provider shall perform an independent audit of its data centers at least annually and at its own expense, and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

13. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

14. Security: The service provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. For example: virus checking and port sniffing — the public jurisdiction and the service provider shall understand each other's roles and responsibilities.

15. Non-Disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

17. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment is the responsibility of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

18. Sub-Contractor Disclosure: The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require the service provider

remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) of XXX hours/ days is met. (XXX shall be negotiated by both parties.)

APPENDIX 2

Guiding Principles

Contracting for XaaS can be confusing. There are different service models using different provider models that create a variety of options to consider. It can be difficult to determine the most appropriate service model. Whether it's a public cloud XaaS solution or private cloud model, a public jurisdiction must also consider a number of internal factors in order to make the best choice. These guiding principles can help as you consider procurement and contracts for XaaS.

1. We can have our cake and eat it too … if we can live with one flavor. XaaS providers offer value and benefits to the public due to scale and a standard business model. Consequently, unique requirements are counter to the model and should be discouraged where possible.

2. The law is the law. Public jurisdictions cannot enter into agreements that violate their laws. Providers and public jurisdictions must understand and respect statutory constraints. If the law truly prohibits a jurisdiction from accepting a particular service provider term or condition, then that term for condition must change or the parties should not engage in a contractual relationship.

3. Want the business? Do what it takes. Public jurisdictions have unique requirements. If a service provider wants this business, it should understand the public environment and offer standard terms and conditions to which public jurisdictions can agree.

4. Not all service providers are created equal. The type of service to be acquired will determine which business model will be most advantageous. Public entities and service providers must work together to ensure they both clearly understand the requirements and share a common understanding of the service model in order to create appropriate contractual terms.

5. Data, data, understand the data. Public jurisdictions must understand and apply an appropriate security classification to their data. Consider the service provider's commitment to secure and protect the data based on the service model. If the service model is not right, don't use it.

6. It takes a partnership. Successful results between government and XaaS providers depend on a clear understanding of the roles and responsibilities of each based on the nature of the service model.

7. All good things must come to an end. Disengagement from the service relationship must be considered prior to the execution of the contract based on the specific service offering.

8. Pick the right dance partner. How well you dance depends on your partner. Picking a partner that is appropriate to your business needs is critical to successful results. Financial viability, maturity, agility, innovation, dependability and proven track record for similar clients are all factors to consider.

9. It's risky business. T&Cs are really about understanding how the public entity and the service provider share and manage risk in their relationship. Success requires a realistic assessment of the risks, a common understanding and a willingness to consider a variety of alternatives to effectively manage those risks.

10. Get by with a little help from your friends. Educate and engage other government policy makers to understand the benefits XaaS providers bring to government and include them early in the process when assessing if traditional contracting, control or auditing practices are the most effective way to protect the public's interest.

11. Trust, but verify. Controls should be commensurate with service provider model, type of data and risk.

APPENDIX 3

Procurement Approaches

Like IT service terms and conditions, sourcing methods have struggled to keep pace with rapidly evolving business technology alternatives driven by cloud service models. Traditional public procurement processes, designed to protect the public's interest, are challenged to find the proper balance between certainty and the flexibility necessary in today's market.

Traditional procurement methods with strict invitation to bid response rules require the proposer to comply with all the requirements of the solicitation or be rejected. These become a "take it or leave it" proposition for service providers. When this kind of sourcing method is used with subscription-based XaaS offerings, which by definition cannot be customized, procurements fail.

Often, traditional models attempt to prescribe solutions. It is important for a state or local government to understand business needs, but XaaS providers frequently limit customization. Prescriptive solutions might be right for some purchases, but not for XaaS. These new service models — driven by ever-changing technology innovation — do not include the purchase of either technology or software. XaaS models include the purchase of services that can be configured to meet the customer's needs, but not customized.

Traditional procurement practices that prevent these new service models from fairly competing deprive governments and their taxpayers of modern, effective tools for managing their increasing digital demands.

Procurement methods are at their core a decision process with objective analytics upon which to base the decision. Decisions should be transparent and competitive, and meet the public jurisdiction's business needs. If procurement processes do not support the acquisition of today's modern services, changes are needed in the practice, rules or statutes.

Here are some approaches or best practices that have improved public procurement results while protecting the public's interest. For some jurisdictions, specific statutes or ordinances may prevent adoption, but there are still useful takeaways from the examples that can help any jurisdiction improve their outcomes for XaaS procurements.

Take Advantage of Negotiations

Evolving business models require the RFP process to be flexible to allow for negotiations or discussions to receive clarification. Some state laws support the process of negotiating terms and conditions in this fashion. California's PCC6611 and Oregon's ORS 279B.060 are good examples of laws that enable a variety of discussion methods. By including the ability to clarify terms and conditions throughout discussions or negotiations, the jurisdiction avoids the problem of rejecting providers that actually might be able to meet the jurisdiction's needs. One typical process is for the jurisdiction to identify certain terms in advance that it is willing to discuss and negotiate before award. By negotiating acceptable terms with the proposer in advance, the jurisdiction ensures it is getting the best fit for the award and resolves differences that otherwise might result in the rejection of an effective proposal.

There are several ways discussions or negotiations may occur. In some cases, the jurisdiction — through the development of its business case and market research — has a good idea of the terms and conditions likely to require negotiation. The jurisdiction can identify those in its RFPs. The jurisdiction can then avoid being forced to reject proposals as nonresponsive that it may otherwise find attractive.

Another way some jurisdictions determine when negotiations may be required is through the issuance of a draft RFP. Feedback from potential proposers can help identify terms that will not work within the market. This gives the jurisdiction the ability to see which terms are problematic and provides the jurisdiction with the option to negotiate. Some RFPs require potential proposers to officially protest specifications they believe are unduly restrictive. This method, while appearing somewhat contentious, can allow the jurisdiction to identify terms and conditions that will be a problem for suppliers and amend the RFP before proposals are submitted. If the jurisdiction does not have the authority to negotiate specific items, that can be plainly made known and help the jurisdiction avoid rejecting otherwise attractive offers.

While Oregon and California may choose to reject a proposal, their laws do not mandate the rejection of a proposal because the proposer takes exception to terms and conditions. It is possible to negotiate terms before final contract award with providers when the law does not require a specific term or condition. Jurisdictions should change their policies, standards and rules to allow for greater use of negotiations in the competitive selection process.

Move Away from Requirements-Based Procurement

Traditional IT system solicitations often rely upon business requirements developed through a series of work sessions that document how the agency currently conducts its business. Getting these requirements perfectly right is a difficult process in the best of circumstances. If successful, these business requirement sessions document the historic business process that may, in itself, be antiquated and inefficient. If those requirements are then made a part of the RFP to be replicated by the service provider, the only solution may be a custom-made solution. This model does not work well for XaaS procurements. Public agencies must understand their business objectives and performance needs, but should not be so prescriptive in their solicitation that they dictate the system design and functionality. Instead, the jurisdiction should be shopping for the best business fit. Rather than evaluate proposals on hundreds or even thousands of prescriptive requirements that may not lead to successful service, public jurisdictions should include evaluation criteria based on how well the service meets or enhances their business objectives, whether it achieves their performance needs and its ability to fine-tune business rules through configuration. Public jurisdictions can make big gains in quality and effectiveness of service in this way through XaaS applications.

Keep Negotiations Moving Forward

A great concern for the parties in any negotiation is how long it will take to reach final agreement. Delays are the enemy of everyone who has a stake in the award of an XaaS contract. Stalled procurements are often caused by long and drawn-out negotiations. Identifying and using generally

agreeable standard terms and conditions at the beginning of the procurement helps limit negotiations to just those terms that are unique and must be tailored to the specific service. It is helpful if all parties do their homework to understand their needs, as well as their partner's needs, before negotiations begin. Successful contracts depend on successful partnerships. Negotiation strategies that find workable solutions that make both parties successful produce the best results over the life of the contract.

Create a Timeline for Negotiations

Setting a realistic timeline for completion of negotiations can help keep negotiations on track and the procurement moving forward. Recently, the Commonwealth of Massachusetts used a tightly defined timeline as an effective tool to keep its award process moving forward. If negotiations were not completed on time, they reserved the right to move to the next proposer. In a recent SaaS procurement, that is exactly what happened. This requires both sides to act responsibly by fulfilling their obligations in a negotiation. It also requires tracking and documenting progress, and the assignment of responsibilities for task completions during negotiations.

Start with a Business Problem-Based Solicitation

The requirements section of a procurement document should always include a background statement that, among other things, defines the business problem to be solved. When the Commonwealth of Massachusetts procured its SaaS procurement system, it started with a business problem-based solicitation. By spending time clearly understanding and articulating the business problem the commonwealth needed to solve, it allowed them to focus on the things the commonwealth was best at and left the range of potential solutions up to the service provider. This approach helps avoid overly prescriptive specifications and encourages innovation and a broader range of solutions on the part of proposers.

Minimize Mandatory Requirements

Delaware's Cloud First Policy is supported by a procurement process that includes SaaS terms and conditions in the RFP as a standard for acceptance. While there is no flexibility on mandatory terms and conditions, the state's preferred terms and conditions are made a part of the RFP. Proposers offering other terms and conditions in lieu of the preferred are reviewed for acceptance by both Delaware Information Technology (DIT) and the agency contracting for the service. The State Procurement Office will only make an award after authorization by DIT. The contractor certifies compliance with the Delaware terms or with approved changes or substitutions and is expected to maintain that compliance through the life of the contract.

RFPs that include mandatory terms that are not negotiable are essentially a "take it or leave it" proposition for providers. If these terms are not acceptable, they can cause an otherwise acceptable proposal to be rejected. Jurisdictions should carefully consider the consequences of using mandatory terms unless it is a requirement of law. Jurisdictions should be certain about the need for a mandatory requirement or term because future negotiations are preempted by their classification as mandatory. The use of mandatory requirements or terms should be kept to an absolute minimum.

Establish Model Terms as Standards

The model terms and conditions could be used as a standard with which service providers certify compliance as a part of the RFP process. If there is agreement on standards, then a selection process can evaluate all potential providers based on reasonable criteria calculated to acceptably manage identified risks and achieve the business needs of client agencies.

Develop National Minimum Standards

The creation of a nationally recognized standard, derived from best practices in XaaS operations — including data handling, data security, confidentiality, availability, etc. — could streamline the procurement of XaaS in state and local governments that use a stricter and customized assessment of responsiveness. It would allow public jurisdictions to evaluate unique proposal offerings against the adopted national standard. By relying on the proposal's certification of compliance against the standard, the procuring organization could use minimum compliance against the standard as the baseline for evaluation of the proposal. Additional functionality beyond the standard could also be used for a more meaningful analysis of "value-added options" or "best value" in an RFP. Requiring the service provider to continue compliance with the standard over the life of the contract also has the benefit of keeping the service current.

Improve Communication

Any effective procurement process for new and evolving business models such as XaaS require a good deal of communication before the issuance of a solicitation, during the solicitation and evaluation, and in contract execution.

Several recent reports and publications underscore the importance of open and effective communication between service providers and the jurisdiction. The need for increased quality and quantity of communication has been called for at all levels of government. The Federal Government's Office of Management and Budget (OMB) issued two memos on this topic headed as "Myth Busting."[25] The IJIS institute called out the importance of communication in improving innovation in public contracting in its December 2013 report.[26] The California Technology Authority is changing procurement practices to remove communication barriers as it implements recommendations of a taskforce formed by the governor and controller to improve technology procurement.[27] Jurisdictions should examine and revise procurement processes, policies and rules wherever possible to eliminate barriers to effective communication.

Conduct Market Research

Jurisdictions that conduct effective market research and share their background information and business needs in open forums with providers before issuing a solution increase their chance for a successful procurement. Dialogue with service providers can help the jurisdiction understand various approaches in the market and how service models work. It can also help test assumptions. Other effective methods of market exploration before issuing a formal solicitation may include issuing a draft RFP to encourage provider comments and responses and holding one-on-one meetings with interested providers. The more a jurisdiction understands what is available in the market and how those solutions might work

for its business needs, the better positioned it is to develop an effective business case and create an effective sourcing strategy. The more service providers understand the needs of the jurisdiction, the better prepared they are to offer the optimal solutions.

This exploratory process can also help the provider and jurisdiction understand when a provider's offering is not a good match for the jurisdiction's business needs. In these cases, effective communication can help both parties be smart about what will and will not work in advance prior to their undertaking the burden of a formal procurement process. Procurement policies and rules should promote the increased use of market research to include public discussion forums, online research, service provider meetings and the sharing of background information.

Use Demonstrations

Often, RFPs include product demonstration scoring. This allows the jurisdiction to evaluate the fit, and to some degree, user acceptance of provider solutions. Demonstrations should be encouraged whenever possible. Washington State and California[28] have successfully used request for demonstration (RFD) sourcing methods to award technology contracts. The scoring of the demonstration determined the award. An RFP typically includes some consideration of costs. With RFD awards, the jurisdiction could also consider cost as a part of the evaluation process. This can be an effective way for end users to test XaaS offerings and for the award decision to reflect the best fit for the jurisdiction's business needs.

This could be coupled with a certification process that invites service providers to pre-certify their agreement to abide by key standards like the model terms and conditions described in this document. Policies, rules and statutes should permit demonstration-based awards.

Implement a Multiple Round Selection Process

The use of multi-step processes, which narrow the field of total responses to a "short list" of final proposals most likely to result in award, can help a jurisdiction be more specific in the second round selection process. During a second round, the use of pilots, demonstrations or supplemental negotiations may result in gaining better clarity as to the fit of the proposed services to the jurisdiction's business needs. It also has the added benefit for the jurisdiction of maintaining a competitive environment.

Permit Multiple Awards

RFP or other sourcing methods may be designed to award to either a single provider or multiple providers. The sourcing document must describe if a single award, multiple awards or some combination will be made. The ability to negotiate final awards with each provider is critical. The solicitation must be clear regarding how awards are determined.

Depending on the need, it may be best for the jurisdiction to identify classes of services it needs and award indefinite delivery/indefinite quantity (IDIQ) contracts to a pool of potential suppliers. Agencies within the jurisdiction may then select suppliers from the pool. Effective use of multiple awards for XaaS applications can be very popular with customer

agencies. It gives them choice and allows them to select from service provider applications that best meet their needs. With rapidly emerging service models, it is a good idea to include the ability to reopen the award process annually to add new providers. Multiple awards that result in contracts for most proposers in the class, rather than just the most competitive, are less controversial, but also may not result in the best pricing. A jurisdiction must consider those tradeoffs in relationship to its acquisition strategy and business case. Texas' recent award of a suite of cloud contracts is an excellent example. Jurisdiction policies, rules and statutes should permit multiple awards.

Create Alternative Sourcing Processes

Some states have the statutory authority to create new sourcing models that do not follow statutory requirements for competitive sealed proposals or invitations to bid. Known as "special procurement," the American Bar Association (ABA) Model Procurement Code sets out a competitive sourcing method that in limited circumstances may be used, "... where the application of all requirements of competitive bidding or competitive proposals is deemed to be contrary to the public interest."[29] Several states, including Alaska, Montana and Oregon have passed similar laws. The flexibility afforded under these statutes allows for the design of accountable and innovative sourcing approaches that are not constrained by traditional source methods. Public jurisdictions should have the ability in rule and statute to permit the development of effective sourcing methods when traditional methods will not work.

New procurement sourcing models must be developed if governments are to take advantage of new service models. Public jurisdictions that support and encourage innovation in procurement processes can benefit from more effective procurement outcomes. Successful solutions should be replicated and shared. Unsuccessful approaches should be evaluated from a lessons learned perspective and then discarded. By incubating and sharing successful procurement models, governments can improve their collective ability to successfully acquire the services they need.

The Importance of Cooperative Contracting Opportunities

In the summer of 2012, formal awards were made to cloud-based XaaS providers that responded to a four-state (Colorado, Montana, Oregon and Utah) cooperative purchase conducted by the Western States Contracting Alliance (WSCA) for GIS cloud services and public cloud services. This first-ever IT services procurement through the WSCA-NASPO Cooperative Purchasing Organization model proved successful with awards to four providers.

The U.S. Communities Purchasing Alliance jointly sponsored by the National Association of Counties, Association of School Business Officials, National Institute of Government Purchasing, the National League of Cities and the U.S. Conference of Mayors offers state and local governments the opportunity to participate and purchase from cloud service contracts. U.S. General Services Administration Schedule 70 Technology Contracts are also available to state and local governments through the cooperative purchasing program.

One of the best opportunities for effective public acquisition of XaaS contracts is with multi-jurisdictional cooperative

procurement. There is no doubt that IT service contracting by public jurisdictions will continue to grow, but one-off contracting processes that complicate service provider responses can limit it.

Smaller jurisdictions potentially stand to benefit from XaaS solutions, yet they can be challenged by lack of resources to put effective sourcing solutions together and come to agreement on terms and conditions. By leveraging multi-jurisdiction teams in the development and award of a menu of XaaS contracts, smaller jurisdictions can efficiently acquire provider solutions that meet their needs and protect their interests.

Cooperative purchases can provide a supplier benefit by aligning disparate jurisdiction purchasers around a common set of terms and conditions and a single master contract award rather than different ones in each jurisdiction. Multi-jurisdiction procurements succeed because providers have a standard acquisition process, terms and conditions, and ordering mechanism to navigate rather than different ones in each jurisdiction. That frees up providers to assist the jurisdiction in selecting the best fit.

Another option is to participate with another jurisdiction in a joint cooperative purchase. A recent example at the state level underscores the value and benefit. In 2014, the State of Texas awarded master IDIQ contracts for IaaS, PaaS, cloud broker and cloud assessment. These contracts are not only available for state agencies and local governments within Texas, but recently the State of Oklahoma signed a joint powers agreement with Texas to purchase from the contracts. This gives Oklahoma agencies a significant range of choices from the Texas contracts and is a great example of collaboration between states.

State laws or local ordinance may prevent a state from "piggy backing" on another jurisdiction's contract, unless they were included in the solicitation at the beginning. Before buying from another jurisdiction's contract, it's a good idea to check local laws to see what is permissible.

As a vehicle for XaaS contracts, multi-jurisdictional cooperative purchasing is an efficient and effective procurement method. It resolves a number of issues in ways that benefit both the participating jurisdiction and providers. Multi-jurisdictional cooperative purchasing:

- Addresses an unmet need for a more organized and effective way to aggregate multiple states' demands for common IT services and commodities. Individual state IT service purchases do not leverage the opportunity of volume buying or contracting efficiencies that come from multi-jurisdiction procurements.
- Aligns with XaaS models. Both cooperative purchasing and XaaS models benefit from consolidated volumes and common approaches to terms and conditions. In this way, one line of code can serve many.
- Creates a contractual mechanism for standard requirements and terms and conditions that help define realistic and practical expectations between public entities and service providers.
- Enables purchases from the cooperative's contract.

Public jurisdictions want the ability to purchase from each other's contracts, but few have the statutory authority to do so without an upfront, coordinated effort. Most states now have authority to participate in cooperative procurements. Cooperative state procurements are typically made available for political subdivisions within the state.

- Provides negotiation leverage for cloud-based solutions through practical and aligned public requirements and aggregated customer volume.

Cooperative purchasing avoids duplication of effort. It leads to greater volume aggregation and typically drives more favorable pricing. With the continued evolution of cloud computing, the aggregation of market demand should provide leverage beyond what an individual jurisdiction could hope to achieve on its own and lead to benefits during this time of market realignment for both state and local governments and service providers.

APPENDIX 4

Lessons Learned Through Cloud Service Procurements

The learning curve can be steep when adopting new business models. With the evolution of cloud service contracts, state and local governments have taken a measured and cautious approach to moving to these new provider models. Over the last year, adoption has increased as a number of state and local governments issue awards for a variety of XaaS models.

Here are several lessons learned from governments that have awarded contracts to XaaS providers. These lessons give others a chance to learn as they develop and execute their XaaS strategy and procurements. They also provide a great source of public jurisdiction contacts.

Delaware

Delaware CIO Jim Sills shared the following lessons. Following a successful Cloud First Policy to "virtualize" all physical servers to create a state private cloud that resulted in greater efficiency and cost savings, Delaware turned its attention to more SaaS applications. The majority of the 70 cloud apps currently deployed in the State of Delaware were acquired through an RFP or by piggy backing on another state contracting vehicle. Over the past three years, the focus has been on apps that leverage the cloud to improve overall "speed to market" and reduce capital outlay expenses. Lessons learned include:

- **Educate your procurement team.** Overall knowledge is key to successful cloud RFPs to acquire cloud solutions.
- **Cloud procurement is a unique process.** It is not "black or white" and is sometimes very complex. Set up dedicated teams to manage the acquisition, as well as the deployments.
- **Understand and realize that cloud touches multiple aspects of IT**, including software, hardware, application development, security, data, networks, architecture and system integrators.
- **It is important to standardize.** Standardize the vetting and terms and conditions process as much as possible to address large and small vendor partner's pain points or barriers.

Georgia

Steve Nichols, chief technology officer for the Georgia Technology Authority, shared lessons from his state's experience developing standards to enable implementation of XaaS cloud solutions within Georgia agencies. Agencies must first request and receive an exemption from a state standard allowing a specific business application to be hosted outside of the state's enterprise data center. Since July 2011, 29 exemptions for XaaS have been approved – virtually all for SaaS. A standard, issued in November 2013, allows agencies to skip the exemption process if the categorization of the data in the as-a-service solution is "low" in the FISMA FIPS-199 sense (confidentiality, integrity, availability), and the system does not need integration points with other state systems. Lessons learned include:

- **Understand the relative value of SaaS provider contracts.** Because many of the SaaS awards are small (low-dollar value), the SaaS providers won't

begin a contract negotiation with a state-generated contract; they will start with their own contract. Georgia found providers are reluctant to change their standard templates for a small contract.

- **Help providers understand state and local government requirements**. Few SaaS providers have dedicated SLED groups (state, local and education) and consequently don't fully understand some of the common practices and limitations on states.
- **Expect differences in help desk support approaches.** Every SaaS provider brings its own set of processes around trouble ticketing, change management, monitoring, etc. Georgia spent several years consolidating and rationalizing all IT service management processes under a common ITIL implementation; every application that goes out to a SaaS vendor can present challenges and confusion by introducing a new and different set of processes.
- **Be prepared for a lack of commonality.** So far, Georgia hasn't seen any commonality among the SaaS procurement. Awards have all been to different providers and all have been structured differently. Given these factors, a statewide contract may be premature at this time.

Massachusetts

Gary Lambert, assistant secretary for operational services, shared the commonwealth's lessons learned in the procurement of a SaaS e-procurement system. The system replaces an e-procurement system that was one of the first in the county. Enterprise system projects can require up to 18 months to negotiate terms and conditions, and the commonwealth needed a fast and successful project that could set an example. Solicited in December 2012, the commonwealth has been under budget and in production since early 2014. Lessons learned include:

- **Focus on the business.** This created some level of difficulty for the team because they have traditionally been used to having a major role in software and hardware issues and IT system design and procurement issues. By moving away from many of the traditional concerns that are the provider's responsibility under a SaaS model, it put the team's focus on making sure their business needs were understood and could be accomplished. The team concentrated on configuration and how to launch, not on software licenses, warranties and upgrades.
- **Set a timeline for negotiation.** To avoid long and drawn out delays, the procurement team should set an aggressive timeline for negotiations. The first provider awarded the contract could not resolve key issues within the eight-week negotiation deadline. Massachusetts moved on to the next proposer who proved capable of meeting its requirements during the time allotted for negotiations.
- **Set a negotiation schedule.** To stay focused and keep issues fresh, negotiations were scheduled every other day. Staff schedules were adjusted to fully engage in negotiations and fulfill their responsibilities for addressing and resolving issues.
- **Make sure key requirements are met.** Section 508 Compliance is taken very seriously in Massachusetts. The first SaaS provider could not meet the requirement and was unlikely to modify its system,

one that historically supported private sector companies that do not have this requirement.

- **Understand the SaaS prime contractor and subcontractor's relationship and responsibilities.** There can be performance and responsibility gaps between a subcontractor responsible for implementation and the prime contractor who simply wants to operate the SaaS. Market research can help understand what models are most common for XaaS. As a public jurisdiction, make sure you are comfortable with the entity subcontracted to accomplish implementation.
- **Remember SaaS is about the business.** Don't put your attorneys at the center of the negotiations. It is about the business. Make sure you know what your business needs are and be confident the service will meet them. Business owners should be intimately engaged in the negotiations, because in the end, their success depends on it.

Oakland County, Michigan

Phil Bertolini, deputy county executive/CIO, and Jim Taylor, chief technology officer, shared the county's lessons. By evaluating application requirements in terms of costs, performance, security and compliance, the county took an evolutionary approach to cloud computing with its expansion of on-premises G2G (government to government) cloud as a shared service. The county wanted to create a cloud environment because it not only provides economic incentives and other benefits to the county, but also to other governments that will access it as customers. Cloud computing resources are now deployed and used where and when it makes sense.

Operational for the past 18 months, the county started by hosting its websites and other government websites, including an application store for the National Association of Counties. Lessons learned include:

- **Benefits can be significant.**
  - » Lower costs and capital expenditures for the county and other governments.
  - » The ability to use and pay for only the computing resources needed because of combined economies of scale from shared computing resources, software and licensing costs.
  - » The pooling of resources in a multi-tenant model allows dynamic assignment and reassignment according to demand.
  - » Faster provisioning and consuming of technology resources.
  - » Improved scalability, redundancy and resiliency; often not available to governments due to lack of financial or technical resources.
  - » Reduced need for the scarce IT resources required to manage servers, networks, security, etc.
- **It will take longer than you think to become fully operational.** With all of the security concerns, contracts, backup/recovery and operational procedures, it just takes time. Plan for it to take longer than you think, especially if you are working with outside entities.
- **Software licensing is key.** When licensing software for use in the cloud, conduct a legal review to make sure you don't violate any of your software license agreements. Some agreements are written for on-premises internal use only. Check with your vendors to ensure you don't

create a compliance issue by moving to the cloud. From a G2G marketplace perspective, Oakland County needed service provider licenses to allow other governments to use internally built software under an as-a service license. You can find more information on this initiative at the G2G cloud solutions website: www.g2gcloud.com and the G2G marketplace website: www.g2gmarket.com.

- **Know how you are getting out BEFORE you get in.** Before you get into the cloud, know how you are going to get out. It is a necessity that you understand and document your cloud environment well enough that if you need to move an application or a cloud environment for any reason, you can. The key is documenting every process and nuance so you know how everything works.
- **Communicate often with internal staff.** The cloud is a new way of doing business, but sometimes staff members feel threatened by its existence. Sometimes employees feel they might lose their jobs or that the value of what they do is now less. Help them understand the cloud is an extension of your internal network and that by learning and understanding the cloud, their value as employees increases rather than decreases. Talk about why your organization is moving to the cloud so employees truly understand your goals. Communicate regularly and often — even if you feel like you are repeating yourself.
- **Know and trust your service provider.** You are in this together through thick and thin. Things are going to come up and you need a partner that is flexible and agile. Above all find a service provider you can trust.
- **Evaluate each application individually for cloud readiness.** Each application is different and some applications might not be well suited for the cloud. Inventory your applications and develop assessment criteria as part of your evaluation. Why should this particular application run in the cloud? Are there any specific security issues like PCI (Payment Card Industry) for taking credit cards or HIPAA (Health Insurance Portability and Accountability Act) that need to be addressed? Oakland County developed a Cloud Readiness Application Template that other governments can use to help identify issues with moving an application to the cloud. A copy of the Cloud Readiness Application Template may be requested by email at info@g2gcloud.com.

Texas

Following a two-year pilot with four agencies intended to reduce server acquisition time and speed up application deployment, Texas awarded master IDIQ contracts for IaaS, PaaS, cloud broker and cloud assessment. Lessons learned include:

- **Service provider service agreements can vary widely and be difficult to compare.** Public jurisdictions should consider developing a template that documents the jurisdiction's minimum terms for cloud services and organizes requirements such as SLAs and availability.
- **Service providers proposed a variety of service levels and some were not adequate to the state's needs.** There are some non-negotiable terms that cannot be changed due to statutory requirements. Public jurisdictions should define service level targets, as well as their tolerance for acceptable ranges of service levels.

- **Service providers have differing abilities to tailor their SLAs and their services to meet specific customer needs.** It is necessary to establish contracts for a range of cloud services with a gradation of service levels to meet the range of customer needs and help customers understand service levels and terms (including, but not limited to, security, ownership and location of data) that service providers offer so they can select the one that best suits their needs.
- **Customers need a plan for return of data at termination and the contract needs to support that right.** Make no exceptions to this contractual requirement.
- **Service providers do not always provide the support, security or risk mitigation that customers may need.** Consider offering options to fill this need through an intermediary (broker or reseller) to provide additional support, security or risk mitigation in addition to agreements with direct service providers.
- **Cloud services contracts can be complex.** Negotiating a cloud service contract has many of the same categories of issues and complexities as negotiating any technology services contract — but there is generally more variety in responses and more complexity in negotiating the final terms. Provide as much upfront planning as possible to structure the expectations and the range of responses. Expect to spend more time in negotiation for these types of contracts.
- **Cloud services are rapidly evolving and there is a lack of standard definitions and terminology.** Public jurisdictions need to encourage the adoption of standard definitions among the vendor and government communities.

APPENDIX 5

Glossary

"Anything as a Service" (XaaS) refers to cloud-based services delivered to customers over the Internet. Typically, the services are purchased on a subscription model. The most common service models used in government today are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), but others are available such as Communications-as-a-Service (CaaS). The service offering will be extensive.

"Authorized Persons" as used in this document means the service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services.

"Data Breach" as used in this document means the unauthorized access by non-authorized person/s that result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

"Individually Identifiable Health Information" as used in this document means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[30]

"Infrastructure-as-a-Service" (IaaS) as used in this document is defined as the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).

"Personal Data" means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g. Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.

"Platform-as-a-Service" (PaaS) as used in this document is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud

infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.[31]

"Protected Health Information" (PHI) as used in this document is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[32]

"Personally Identifiable Information" (PII) No one definition applies to all states. Generally, PII refers to a combination of data elements (e.g. Social Security number, driver's license or other government-issued identification number, passport number, financial account number, or credit or debit card number in combination with security codes) that, when linked to the individual's first name or first initial and their last name, and not encrypted or otherwise could lead to the loss, theft or unauthorized use of the individual's personal information.

"Public Jurisdiction" as used in this document means any government or government agency that uses these terms and conditions.

"Public Jurisdiction Data" as used in this document means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware; the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

"Security Incident" means the potentially unauthorized access by non-authorized persons to personal data or non-public data that could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of a service provider. A security incident may or may not turn into a data breach.

"Service Level Agreement" (SLA) means a written agreement between both the public jurisdiction and the service provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises (i.e., metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed and (6) any remedies for performance failures.

"Service Provider" means the contractor, their employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

"Software-as-a-Service" (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[33]

"Statement of Work" is a written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

APPENDIX 6

Clause Comparison Matrix

Plain Language	SaaS	PaaS	IaaS
1. Definition of terms. Defines the service model and terms used.	**1. Software-as-a-Service (SaaS)** as used in this document is defined as the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	**1. Platform-as-a-Service (PaaS)** as used in this document is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.	**1. Infrastructure-as-a-Service (IaaS)** as used in this document is defined as the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).
2. The public jurisdiction owns all of its data. The service provider will not access the data except as needed to do the work of the contract.	**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the public jurisdiction's written request.	**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts, or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the public jurisdiction's written request.	**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts, or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the public jurisdiction's written request.

Plain Language	SaaS	PaaS	IaaS
3. The public jurisdiction owns all personal information. The service provider will protect it and will not use the data for anything not related to the customer. The service provider will encrypt personal data and non-public data both at rest and in transit.	**3. Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions: a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. b. All data obtained by the service provider in the performance of this contract shall become and remain property of the public jurisdiction. c. All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of this contract. d. Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit. The public jurisdiction shall identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. e. At no time shall any data or processes – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees – be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction. f. The service provider shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.	**3. Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions: a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction. c. Unless otherwise stipulated, personal data and non-public data shall be encrypted at rest and in transit with controlled access. The service level agreement (SLA) and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control. d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. e. At no time shall any data or processes – which either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees – be copied, disclosed, or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.	**3. Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions: a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction. c. Unless otherwise stipulated, personal data and non-public data shall be encrypted at rest and in transit with controlled access. The service level agreement (SLA) and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control. d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. e. At no time shall any data or processes – which either belong to or are intended for the use of public jurisdiction or its officers, agents or employees – be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

Plain Language	SaaS	PaaS	IaaS
4. The service provider will not store any of the public jurisdiction's non-public data outside the U.S.	**4. Data Location:** The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.	**4. Data Location:** The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.	**4. Data Location:** The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.
5. The service provider will notify the public jurisdiction of a security breach. In the case of a SaaS or PaaS, the service provider will notify the public jurisdiction of a security incident.	**5. Security Incident or Data Breach Notification:** The service provider shall inform the public jurisdiction of any security incident or data breach. **a. Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract. **b. Security Incident Reporting Requirements**: The service provider shall report a security incident to the appropriate public jurisdiction identified contact immediately as defined in the SLA. **c. Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.	**5. Security Incident or Data Breach Notification:** The service provider shall inform the public jurisdiction of any security incident or data breach within the possession and control of the service provider and related to service provided under this contract. **a. Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed, defined by law or contained in the contract. **b. Security Incident Reporting Requirements:** Unless otherwise stipulated, the service provider shall immediately report a security incident related to its service under the contract to the appropriate public jurisdiction identified contact as defined in the SLA. **c. Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.	**5. Security Incident or Data Breach Notification:** The service provider shall inform the public jurisdiction of any security incident or data breach related to public jurisdiction data within the possession or control of the service provider and related to the service provided under this contract. **a. Security Incident Reporting Requirements:** Unless otherwise stipulated, the service provider shall immediately report a security incident related to its service under the contract to the appropriate public jurisdiction identified contact as defined in the SLA. **b. Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall (1) promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

Plain Language	SaaS	PaaS	IaaS
6. If a service provider is responsible for a breach, they will pay the cost of the breach investigation, resolution, notification, credit monitoring and call centers up to a set amount per record/ per person. The service provider will take corrective action subject to any limitation of liability in the contract.	**6. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of service provider. a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident. b. The service provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary. c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law – all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/ person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute[34] at the time of the data breach; and (5) complete all corrective actions as reasonably determined by service provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.	**6. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider and related to the service provided under this contract. a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident. b. The service provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary. c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law; all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute[35] at the time of the data breach; and (v) complete all corrective actions as reasonably determined by service provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.	**6. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of a service provider and related to service provided under this contract. a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident. b. The service provider, unless stipulated otherwise, shall promptly notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary. c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) a website or a toll-free number and call center for affected individuals required by state law; all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/ person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute[36] at the time of the data breach; and (5) complete all corrective actions as reasonably determined by the service provider based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.

Plain Language	SaaS	PaaS	IaaS
7. The service provider will notify the public jurisdiction of any legal requests that might require access to the public jurisdiction's data.	**7. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.	**7. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.	**7. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.
8. The service provider will not erase the public jurisdiction's data in the event of a suspension or when the contract is terminated. Specific time periods are established where data will be preserved by the service provider based on the circumstances of termination and the type of service provided. The service provider will destroy data using a NIST-approved method when requested by the public jurisdiction.	**8. Termination and Suspension of Service:** a. In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data in a CSV or another mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of public jurisdiction data. b. During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data. c. In the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of: • 10 days after the effective date of termination, if the termination is in accordance with the contract period • 30 days after the effective date of termination, if the termination is for convenience • 60 days after the effective date of termination, if the termination is for cause After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. d. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the SLA. e. The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.	**8. Termination and Suspension of Service:** a. In the event of an early termination of the contract, the service provider shall allow for the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content. b. During any period of suspension, the service provider shall not take any action to intentionally erase any public jurisdiction digital content. c. In the event of early termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of: 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the service provider will impose no fees for access and retrieval of digital content to the customer. d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all of its forms, such as disk, CD/DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.	**8. Termination and Suspension of Service:** a. In the event of an early termination of the contract, the service provider shall allow for the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content. b. During any period of suspension, the service provider shall not take any action to intentionally erase any public jurisdiction digital content. c. In the event of early termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the service provider will impose no fees for access and retrieval of digital content to the customer. d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all of its forms, such as disk, CD/DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST- approved methods. Certificates of destruction shall be provided to the public jurisdiction.

Plain Language	SaaS	PaaS	IaaS
9. The service provider will perform background checks on staff, including subcontractors. The service provider will not use staff who have criminal convictions.	**9. Background Checks:** The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.	**9. Background Checks:** The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.	**9. Background Checks:** The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.
10. The service provider will provide reports to the public jurisdiction for its accounts in a format agreed to in the SLA. The reports include: latency statistic, user access, user access IP addresses, user access history and security logs.	**10. Access to Security Logs and Reports:** The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA agreed to by both the service provider and the public jurisdiction. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this contract.	**10. Access to Security Logs and Reports:** a. The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA and agreed to by both the service provider and the public jurisdiction. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this contract. b. The service provider and the public jurisdiction recognize that security responsibilities are shared. The service provider is responsible for providing a secure infrastructure. The public jurisdiction is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.	**10. Access to Security Logs and Reports:** a. The service provider shall provide reports to the public jurisdiction directly related to the infrastructure that the service provider controls upon which the public jurisdiction account resides. Unless otherwise agreed to in the SLA, the service provider shall provide the public jurisdiction a history or all API calls for the public jurisdiction account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the service provider. The report will be sufficient to enable the public jurisdiction to perform security analysis, resource change tracking and compliance auditing. b. The service provider and the public jurisdiction recognize that security responsibilities are shared. The service provider is responsible for providing a secure infrastructure. The public jurisdiction is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.
11. The public jurisdiction can audit conformance to contract terms.	**11. Contract Audit:** The service provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense.	**11. Contract Audit:** The service provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense.	**11. Contract Audit:** The service provider shall allow the public jurisdiction to audit conformance to the contract terms. The public jurisdiction may perform this audit or contract with a third party at its discretion and at the public jurisdiction's expense.

Plain Language	SaaS	PaaS	IaaS
12. The service provider will have an independent audit performed of its data centers annually.	**12. Data Center Audit:** The service provider shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.	**12. Data Center Audit:** The service provider shall perform an independent audit of its data centers at least annually and at its own expense, and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.	**12. Data Center Audit:** The service provider shall perform an independent audit of its data centers at least annually and at its own expense, and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.
13. The service provider will notify the public jurisdiction of upgrades and maintenance.	**13. Change Control and Advance Notice:** The service provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.	**13. Change Control and Advance Notice:** The service provider shall give advance notice (to be determined at contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.	**13. Change Control and Advance Notice:** The service provider shall give advance notice (to be determined at contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.
14. The service provider will disclose security processes and technical limitations.	**14. Security:** The service provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. For example: virus checking and port sniffing – the public jurisdiction and the service provider shall understand each other's roles and responsibilities.	**14. Security:** The service provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. For example: virus checking and port sniffing – the public jurisdiction and the service provider shall understand each other's roles and responsibilities.	**14. Security:** The service provider shall disclose its non-proprietary security processes and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. For example: virus checking and port sniffing – the public jurisdiction and the service provider shall understand each other's roles and responsibilities.
15. The service provider will limit staff knowledge of data and separate duties to protect the data. Non-disclosure agreements are required of service provider staff.	**15. Non-disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.	**15. Non-disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.	**15. Non-disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.
16. The public jurisdiction can import or export its data whenever needed.	**16. Import and Export of Data:** The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers.	**16. Import and Export of Data:** The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers.	**16. Import and Export of Data:** The public jurisdiction shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

Plain Language	SaaS	PaaS	IaaS
17. The service provider is responsible for all hardware, software, personnel and facilities needed to deliver services. Service will be available 24/7.	**17. Responsibilities and Uptime Guarantee:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing, and maintaining the environments are the responsibilities of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.	**17. Responsibilities and Uptime Guarantee:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment is the responsibility of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.	**17. Responsibilities and Uptime Guarantee:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment is the responsibility of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.
18. The service provider will disclose all subcontractors.	**18. Subcontractor Disclosure:** The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.	**18. Subcontractor Disclosure:** The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who will be involved in any application development and/or operations.	**18. Subcontractor Disclosure:** The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.
19. The public jurisdiction may have the service provider remove staff.	**19. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.	**19. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.	**19. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.
20. When asked by the public jurisdiction, the service provider will provide business continuity and disaster recovery plans. Both parties must agree on recovery time objectives (RTO) in the contract. The service provider will meet the RTOs.	**20. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)	**20. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)	**20. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)

Plain Language	SaaS	PaaS	IaaS
21. The service provider will comply with accessibility requirements.	**21. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.	**21. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.	No corresponding clause – not relevant to service model. Standards would be selected by the public jurisdiction.
22. The service provider will use Web services where possible to interface with public jurisdiction data.	**22. Web Services:** The service provider shall use Web services exclusively to interface with the public jurisdiction's data in near real time when possible.	**22. Web Services:** The service provider shall use Web services exclusively to interface with the public jurisdiction's data in near real time when possible.	No corresponding clause – not relevant to service model. Standards would be selected by the public jurisdiction.
23. The service provider will encrypt data at rest and data that resides on mobile devices.	**23. Encryption of Data at Rest:** The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data, unless the public jurisdiction approves the storage of personal data on a service provider portable device in order to accomplish work as defined in the statement of work.	**23. Encryption of Data at Rest:** The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Sensitive personal data, unless the service provider presents a justifiable position that is approved by the public jurisdiction that sensitive personal data, is required to be stored on a service provider portable device in order to accomplish work as defined in the scope of work.	No corresponding clause – not relevant to service model. Standards would be selected by the public jurisdiction.

ENDNOTES

1. Special Publication 800-145, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, September 2011.
2. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, September 2012
3. Ibid.
4. Ibid.
5. State Security Breach Notifications Laws, National Conference of State Legislatures, website, April 11, 2014.
6. P2-1, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," Special Publication 800-122, National Institute of Standards and Technology, April 2010.
7. P5, "Data Security Breach Notification Laws," Gina Stevens, Congressional Research Service, April 10, 2012.
8. P11, "There is a New Sheriff in Town; The Auditor, Internal Controls and You," Contract Management, September 2006, Richard Pennington J.D.
9. P1, "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute Research Report, May 2014.
10. P2-3, NIST SP 800-111, "Guide to Storage Encryption Technology for End-User Devices," November 2007.
11. FIPS 140-2 issued by the National Institute of Standards and Technology defines four levels of security.
12. The COSO identified five potential benefits in its 2012 paper, "Thought Leadership in ERM: Enterprise Risk Management for Cloud Computing," including cost savings – pay only for the resources used; speed of deployment – time to fulfill requests for computing power and application can decrease from months to weeks, weeks to days, and days to hours; scalability and better alignment of technology resources – allows and organization to scale capacity up and down from one server to one hundred services without capital expenditure; decreased effort in managing technology – allows internal IT functions to focus on core goals; and environmental benefits-reduced power consumption and carbon footprint
13. Examples of third-party audits: Service Oriented Control (SOC), SOC 2 and SOC 3 report against a baseline of trusted principles and criteria addressing security, availability, processing, confidentiality and privacy established by the American Institute of CPAs.
14. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health.
15. U.S. Department of Health and Human Services, National Institute of Health, HIPAA Privacy Rule, Definitions.
16. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations" National Institute of Standards and Technology, May 2012.
17. "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013
18. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health.
19. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, May 2012.
20. U.S. Department of Health and Human Services, National Institute of Health, HIPAA Privacy Rule, Definitions.
21. "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013
22. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health.
23. U.S. Department of Health and Human Services, National Institute of Health, HIPAA Privacy Rule, Definitions.
24. "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013.
25. "Myth-Busting: Addressing Misconceptions to Improve Communications with Industry During the Acquisition Process," Daniel I. Gordon, February 2, 2011, OMB, and "Myth Busting: Addressing Misconceptions and Further Improving Communications During the Acquisition Process," OMB, May 7, 2012.
26. "Strategies for Procurement Innovation and Reform," IJIS Institute, December 10, 2013.
27. P24, "Recommendations to Improve Large Information Technology Procurements: A Road Map for Success in California," Task Force on Reengineering IT Procurement for Success, August 2013.
28. P31-32, "Seeing Excellence: Learning from Great Procurement Teams," Richard Pennington, 2013.
29. Section 3-207, The 2000 Model Procurement Code for State and Local Governments, American Bar Association.
30. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health.
31. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, May 2012.
32. U.S. Department of Health and Human Services, National Institute of Health, HIPAA Privacy Rule, Definitions.
33. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, May 2012.
34. "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013.
35. Ibid.
36. Ibid.