SMART GRID INTEROPERABILITY PANEL

Cloud Computing Considerations in the Smart Grid

Assessing and Implementing Cloud Computing Initiatives that Potentially Impact the Smart Grid

Document Source: Smart Grid Cybersecurity Committee Cloud Computing Subgroup
Author/Editor: Elizabeth Sisley et al.
Production Date: November 2014, V. 25

Disclaimers

- The information contained in this document is the proprietary and exclusive property of SGIP 2.0, Inc. (SGIP) except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes without the prior written permission of SGIP.
- The information contained in this document is subject to change without notice.
- The information in this document is provided for informational purposes only. SGIP specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.
- This document adheres to the SGIP Intellectual Property Rights (IPR) Policy.

Smart Grid Interoperability Panel

The Smart Grid Interoperability Panel (SGIP) is a public-private non-profit collaborative working to identify requirements for interoperability and technical standards. SGIP members work together to accelerate interoperability, testing and certification so that efficient, secure electrical power can reliably maintain and increase standards of living around the world. Members also have privileged access to the collected knowledge and expertise of all the domains in the smart grid ecosystem. To learn more about SGIP, visit http://sgip.org/.

Contents

1 Executive Summary

Cloud computing, a method of configuring and delivering computing power on demand, is growing rapidly. Analysts project that almost 90 percent of new spending over the next six years on Internet and communications technologies, a $5 trillion global business, will be on cloud-based technology.[1]

The smart grid, which integrates information and communication technologies with the delivery of electricity over the power grid, is making increasing use of cloud computing. One recent report estimated that annual utility spending in smart grid as a service, one example of the way in which utilities are using cloud-based services, will grow from $1.7 billion worldwide in 2014 to $11.2 billion in 2023–totaling $57.6 billion over that time period.[2]

For the smart grid community—including system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services—there are a number of important considerations to keep in mind when using cloud computing for the smart grid.

The goals for this paper are to:

1. Introduce background material on cloud computing and its essential characteristics.
2. Communicate the smart grid options for cloud services.
3. Discuss how the risks may or may not differ when cloud services are used (e.g., privacy for Advanced Metering Infrastructure (AMI), employee issues, data ownership, etc.)
4. Discuss SLA priority requirements such as availability, security, and auditing of the service provider.

According to NIST Special Publication (SP) 800-145, *The National Institute of Standards and Technology (NIST) Definition of Cloud Computing*: [3]

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."*

[1] "The Era of Cloud Computing," New York Times, June 2014, http://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/?_php=true&_type=blogs&_r=0.

[2] "Smart Grid as a Service: Managed Services for Home Energy Management, AMI, DA and SA Communications, Substation Asset Monitoring, Demand Response, and IT Systems and Analytics," Navigant Research, May 2014, http://www.navigantresearch.com/research/smart-grid-as-a-service .

[3] NIST SP 800-145 provides more detail regarding these definitions, and also defines a list of characteristics that have commonly been considered essential to a Cloud definition. NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, expands on these definitions, and provides a detailed discussion of topics that should be considered for each of the deployment scenarios and standard service categories.

The five essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[4] The three service models are software, platform, and infrastructure.

1. **Software as a Service (SaaS)** is a software distribution model in which applications are hosted by a service provider and made available to customers over a network, typically the Internet.
2. **Platform as a Service (PaaS)** is a paradigm for delivering operating systems and associated services over the Internet without downloads or installation.
3. **Infrastructure as a Service (IaaS)** involves outsourcing the equipment used to support operations, including storage, hardware, servers, and networking components.

Cloud Service Providers (CSPs) may have more rigorous best practices than an organization's internal implementation of a cloud environment, as they are specializing their business practices around cloud services. However, CSPs still need to be monitored and managed, and issues documented in contracts and SLAs. CSPs should be considered as *managed service providers*, and the utility should actively manage such a provider in order to ensure the quality of services received. It is important that the procurement process includes a Service Level Agreement (SLA) that defines the utility's requirements that the CSP must meet, as in any other managed service relationship.

This white paper was prepared by the Cloud Computing Subgroup of the SGIP's Smart Grid Cybersecurity Committee (SGCC). This subgroup addresses the unique cybersecurity issues of using and managing smart grid applications that utilize the cloud.

2 Cloud Computing in the Context of the Smart Grid

In its purest form, cloud computing relies on a centralized infrastructure that provides the equipment, space, and bandwidth to support a variety of computing services to a large number of consumers. CSPs may employ a variety of customer agreements that include demand-based pricing, capacity reservation, and other measures to help mitigate demand peaks and enhance revenue. Consumers (i.e., utilities, in this white paper) may be able to time shift some demand either on an ad-hoc basis (e.g., running a data analysis process on historical data early to capture price breaks) or on a planned basis (e.g., designing a system to use batch jobs to shift some demand to off-peak time periods). Part of the value of cloud computing is the multitude of ways in which it can be implemented.

2.1 Cloud Computing Deployment and Categories of Services

The following figure presents an overview of the NIST cloud computing reference architecture, which identifies the major actors, their activities and functions in cloud computing. The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing.

[4] Full definitions of these terms may be found in NIST SP 800-145.

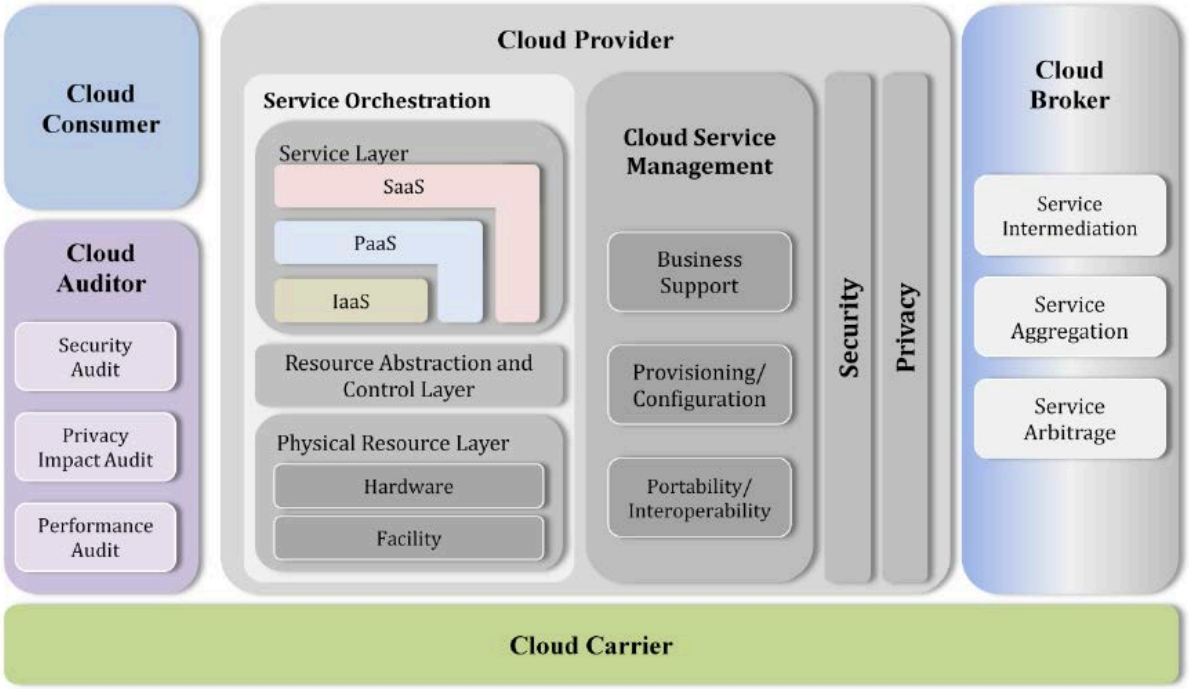

Figure 1: The Cloud Conceptual Reference Model[5]

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Table 1 - Actors in the Cloud Computing Conceptual Reference Model

As shown in Figure 1, the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing. Note that it is the Service Layers that define the differences in categories or types of services as described in Section 2.1.2. The remaining functionality and services support any of the categories/types of services: SaaS, PaaS, or IaaS.

[5] Special Publication 500-292, *NIST Cloud Computing Reference Architecture.* http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

The services of security and privacy are intended to be fundamental to data on the cloud, and traditionally are drawn as cross-cutting services that provide end-to-end support. For example, one utility might be willing to put data in the cloud if the *utility* controlled the security and encryption around that data. A utility's requirements of Confidentiality, Integrity, and Availability (CIA) will still need to be met, because the utility should not delegate all control of their information over to the CSP.

The diagram also shows the additional services beyond the service layers (SaaS, PaaS, or IaaS) that need to be provided to be a complete cloud environment.

A telecommunications carrier, represented as a Cloud Carrier in Figure 1, may provide data transport only, or may be combined with a cloud provider to bundle services as is done in the SaaS, PaaS, and IaaS choices. If the telecommunications carrier and the Cloud Carrier are different legal entities, the utility requirements in the SLA and the overall contract need to be adequately addressed in any subcontracting between the cloud provider and the carrier(s).

2.1.1 Deployment Models

The control of a cloud computing environment is described by the four common deployment models taken directly from NIST SP 800-145:

1. **Private cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers of cloud services (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2. **Community cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
3. **Public cloud:** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
4. **Hybrid cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2.1.2 Categories/Types of Services

The standard categories of services available from cloud providers may be described by the following three models, also from NIST SP 800-145:

1. **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either 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.

2. **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. 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 configuration settings for the application-hosting environment.
3. **Infrastructure as a Service (IaaS):** 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, and deployed applications.

3 Applications of Cloud Computing in the Smart Grid

The smart grid is "a modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications."[6] The smart grid consists of seven domains, which are high-level groupings of organizations, buildings, individuals, systems, devices, or other actors with similar objectives and relying on—or participating in— similar types of applications. The various actors are needed to transmit, store, edit, and process the information needed within the smart grid, and are documented in the NIST Interagency Report (NISTIR) 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity*.[7]

Each of the domains of the smart grid is composed of actors (devices, systems, or programs that make decisions and exchange information necessary for executing applications within the smart grid) and the logical interfaces between actors (including the general types of information exchanged but not including specifications or protocols) that connect them. There is an opportunity to leverage a cloud computing model in the smart grid, but it is critical that cybersecurity practices from both cloud computing and smart grid are applied.

Core tenants of cloud computing such as hosting, services, and distributed communications continue to expand, driven by the potential of reduced costs and the promise of a secure and reliable computing capability with less in-house resources required. However, the use of such distributed capabilities for smart grid applications means that there may be both direct and some indirect two-way transactions between the infrastructure and non-infrastructure (such as back office billing) components. The potential for such interactions to negatively impact associated control systems, infrastructure components, and processes means that smart grid cloud

[6] *Smart Grid: A Beginner's Guide* at p. 3, available at http://www.nist.gov/smartgrid/upload/SmartGrid_guide.pdf.
[7] NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity*, available at http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

computing deployment initiatives should be carefully analyzed to ensure availability, integrity, and confidentiality of data and services are preserved.

3.1 Relevant Cloud Computing Vulnerabilities

The cybersecurity requirements documented in NISTIR 7628 are applicable when considering a cloud implementation for smart grid systems, although some of the risks may change if part of the utility's business process is implemented in a cloud environment. Many of the risks remain the same. However, it is important to note that the analysis conducted in preparation of this white paper showed that there was an increase in the level of risk for those risks that changed when implemented in a cloud environment.

Migrating some of a utility's business processes to a cloud environment is a paradigm shift in thinking. When making a decision to migrate part of their business process, a utility should first consider the potential to impact operations and the delivery of critical services. If there is an added value by migrating a business process to a cloud environment, the utility can then evaluate how the CSP provides security, data ownership, and trust. Since a CSP is a service provider, the utility should be willing to actively manage their chosen CSP.

Some aspects of cloud environments are unique, and not traditionally topics that utilities have needed to deal with. One of the key changes in the migration to a cloud environment is *control of data*:

- Data ownership: The issue of who owns the data[8] is key, and the utility should understand that if the CSP puts into a contract that they own the data, then that data no longer belongs to either a utility or the customer receiving the energy services. As a result, the privacy of the energy customer could potentially be compromised, and it is the utility's responsibility to protect the energy customer data under its control. A cloud provider would be considered a contracted agent, and therefore may be held liable to provide minimum cybersecurity and privacy services equal to what the utility implements.[9]
- Privacy impact assessment (PIA): A privacy impact assessment (PIA) is a comprehensive process for determining the privacy, confidentiality, and cybersecurity risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate identified risks.[10] All risks cannot be eliminated, but all can be mitigated to some degree. Potential risk mitigation activities include: Risk acceptance, risk avoidance, risk mitigation, risk sharing, risk transference, or a combination of these.[11] A PIA should be conducted with the cybersecurity risk assessment when a new system is being developed, as well as when there is a major change to a system, physical component, or within operations that may impact how data is handled and accessed. For example, the

[8] The Third Party Doctrine may be applicable in these instances. For a discussion on the Third Party Doctrine, please see http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

[9] Per legal analysis from Microsoft (accessed from http://technet.microsoft.com/en-us/magazine/hh994647.aspx on June 27, 2014): "In the United States, both federal and state government agencies such as the FTC and various attorneys general have made enterprises accountable for the actions of their subcontractors. This has been replicated elsewhere, such as in the EU with the data protection agencies."

[10] NISTIR 7628, Volume 2, Chapter 5.

[11] See DOE Risk Management Process, RMP, Section 3.3.2.1 for further detail.

advanced metering infrastructure (AMI) is a part of the smart grid that has customer privacy concerns because energy usage data can potentially be personal information. Conducting a PIA is critical to protecting consumer privacy, especially when customer data will be residing in systems external to the utility.

- Derivative data: Another issue is who owns derivative data, for example, the public domain data or metadata that potentially can be mixed in with a utility's data, such as homeowner's name and address, in addition to such data as energy usage at specific locations. Utility data should be stripped of identifying content, but sometimes the derivative data is missed or left in a system because it is considered public domain data, and hence public knowledge.
- Privacy notifications: The legal relationship between the utility and any external parties determines when privacy notifications should be issued directly to energy consumers and what they should contain. In some cases, there are legal requirements that determine the frequency and content of privacy notifications.
- Secondary purpose: A secondary purpose is using energy customer data for additional purposes beyond those for which the data was collected, such as to offer insurance for customer-owned equipment. Permission should be obtained from energy customers to use data for any secondary purpose. In some states, such as California, it is a legal requirement.

All of these are subject to approval by the appropriate regulatory authority, often a Public Utility Commission or Public Service Commission.

It is the utility's responsibility to ensure that the CSP fulfills the cybersecurity and privacy requirements. In planning the cloud architecture, all components should be vetted to confirm that private information/data is not being released. A privacy impact assessment (PIA) would identify potential risks.

3.2 Applying the NESCOR Failure Scenarios to Cloud Computing

The Electric Power Research Institute's (EPRI's) National Electric Sector Cybersecurity Organization Resource (NESCOR) project documented a number of failure scenarios in a whitepaper.[12] This cloud whitepaper leverages the NESCOR failure scenarios and expands on them by describing the likely changes in risk if part of the AMI business process (data and control between meters, headend, and the utility's Customer Information, Energy Management, and Meter Data Management systems) is implemented in a cloud environment.

Most of the risks are the same with or without a cloud implementation, but the following changes in risk also need to be addressed in an SLA:

- All of the possible risks involving employees are still valid, with the addition of less utility awareness into or control of the behavior of the cloud provider's employees.
- If cryptography is managed by the CSP, the utility does not have the ability to manage or control the cryptography. A utility may prefer to control or require a specific encryption method and not delegate it to the cloud provider, thus retaining

[12] *Electric Sector Failure Scenarios and Impact Analyses*, EPRI NESCOR, September 2013.

responsibility and liability. Both provider and utility may need to perform key management, which may add complexity if this were to cause duplication of functionality.

- There is no change in risk for alarms from meters, but a greater risk of external spoofing exists as the meter data is no longer in an utility-owned system. Any time data passes into or out of the cloud environment, the confidentiality, integrity, and availability of that data needs to be considered. Depending on the application or the kind of data, one or more of the tenets can be considered as not "critical." For example, if the metering data becomes unavailable for 15 minutes, it is likely not to have much adverse impact.

In some cases, the level of risk may be increased if/when part of the utility's business process is implemented in a cloud environment. Even if the risks are the same, the SLA should define *when* and *how* the CSP has the liability to repair and recover functionality.

3.3 Steps to Creating an Effective SLA for Cloud Computing

Many of the technical details in these steps can be determined by following the NISTIR 7628 User's Guide[13] process, and leveraging both the NIST Cloud Computing Reference Architecture[14] and Cloud Service Level Agreement (SLA) best practices as needed.

The Cloud Standards Customer Council, an end user advocacy group dedicated to accelerating cloud's successful adoption, provides cloud consumers (utilities) with the steps to take when evaluating cloud SLAs to help them understand what to expect when comparing CSPs or negotiating terms with a provider, as detailed in the *Practical Guide to Cloud Service Level Agreements, Version 1.0*.[15]

Best practices for procurement[16] from the Energy Sector Control Systems Working Group (ESCSWG) offer additional guidance for evaluating and contracting for software and services, with a focus on cybersecurity. The following are the key requirements to evaluate how cloud architectures may impact the risks, and are expanded upon in Table 1, SLA data policies in the *Practical Guide to Cloud Service Level Agreements*.

- Data Preservation - Timely and efficient capturing and preservation of data allow informed addressing of operational, strategic, and litigious situations. Service support should include sources, scheduling, backup, restore, and integrity checks.
- Data Redundancy - Redundancy should be designed to address business needs, and can be tested to demonstrate service availability. The utility should review the protections offered or omitted by the CSP's SLA.
- Data Location - The utility should consider how the SLA will complement their data management strategy, including where the data will reside, where it is processed, and how this meets regulatory requirements.

[13] Available at http://sgip.org/NISTIR-7628-User-s-Guide---Smart-Grid-Cyber-Security-Implementation-Guidelines.
[14] *NIST Cloud Computing Reference Architecture*, Special Publication 500-292, September 2011.
[15] http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf.
[16] *Cybersecurity Procurement Language for Energy Delivery Systems*, Energy Sector Control Systems Working Group, April 2014.

- Data Seizure via subpoena or other legal method - The SLA should address possible legal seizure, as well as what arrangements are in place to obtain the data should the CSP go out of business.
- Data Privacy - The SLA should include the CSP's data privacy policy, and define the data sets gathered, data retention policies, how the data is communicated, and how personal data is stored and used.

Step 1: Identify the Cloud Actors

The NIST Cloud Reference Architecture [14] identifies five unique cloud actors:

- ***Cloud Consumer (Utility).*** The person or organization that maintains a business relationship with, and uses service from, cloud providers. This white paper addresses cloud consumers that are utilities, while referenced documents have a broader definition.
- ***Cloud Provider.*** The person, organization, or entity responsible for making a service available to cloud consumers.
- ***Cloud Carrier.*** The intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.
- ***Cloud Broker.*** An organization that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.
- ***Cloud Auditor.*** A party that can conduct independent assessments of cloud services, information system operations, performance, and security of the cloud implementation.

For the purpose of this document, the utility is the Cloud Consumer, and the Cloud Provider is assumed to be the CSP. The Cloud Carrier's functionality is assumed to be provided by the Cloud Provider, either directly or via a subcontract. The other Cloud actors are beyond the scope of this paper. Each actor has a unique role and responsibilities. Only the first three, Consumer, Provider, and Carrier, have relationships with one another regarding the terms and conditions in the SLAs.

Step 2: Evaluate Business-Level Policies

The policies expressed in the SLA should be evaluated against the utility's business strategy and policies. The data policies that utilities need to consider for inclusion in the cloud SLA when reviewing a cloud SLA are data preservation, redundancy, location, seizure, and privacy.

The business-level policies that should be considered for inclusion in the SLA include guarantees, list of services not covered, excess usage, payment and penalty methods, subcontracted services, licensed software, and industry specific standards. Details are documented in Table 2, SLA business-level policies in the *Practical Guide to Cloud SLAs.*

Step 3: Understand SaaS, PaaS and IaaS

The third step is to understand what SaaS, PaaS, and IaaS are about, and which type of cloud it is running on (private, public, or hybrid). Terms and conditions in the SLA depend on the complexity of control variables that the CSP gives to the Cloud Consumers. Details on SaaS, PaaS, and IaaS are provided in Section 2.

The SLA for SaaS is typically not as complex as the SLA for PaaS. The only control the SaaS consumer (end users) has is to access the SaaS application, while the PaaS consumers (developers) have controls over the application development life cycle but not the virtual machines. The SLA for the IaaS is typically the most complex, as the IaaS consumers (infrastructure specialists) have control over the virtual machines but not physical infrastructure.

Step 4: Identify Critical Performance Objectives

The fourth step is to identify what metrics should be used to achieve performance objectives. The key metrics for a cloud environment are efficiency and accuracy of service delivery. A risk-based approach can be useful in identifying the unique performance objectives of the utility's services, and the *NISTIR 7628 User's Guide* documents such a process.[13]

Performance metrics often include: availability, response time, transaction rate, and processing speed. Utility-specific metrics are also important, to ensure that migrating part of the utility's business process to a cloud environment does not degrade service to the energy customers. Cybersecurity metrics should be specified, and NISTIR 7628 provides additional guidance on identifying applicable security requirements.

Step 5: Evaluate Security and Privacy Requirements

See NISTIR 7628 User's Guide for a methodology to identify, select, and assess the applicable security and privacy requirements for a smart grid information system. Consider including key security and privacy requirements within cloud SLAs, such as:

- Asset sensitivity. The more sensitive the data, the more security and privacy safeguards that must be in place.
- Legal/regulatory requirements. Ensure the CSP complies with all of the utility's applicable legal requirements to protect the data, and that they have a breach response plan in place in the event data is lost, stolen, or accessed in unauthorized ways.
- CSP's security capabilities. Include the right to audit the CSP's security and privacy program, and/or require an independent third-party audit.
- Seizure via subpoena or other legal method. Include the steps the CSP must take in the event they receive a legal request to access utility data. Typically they should contact the utility before turning over any data.
- NOTE: Currently privacy is primarily a requirement in the AMI domain, as the other domains rarely have customer data. However, as the smart grid evolves, this situation may change. This will be even more likely as big data analysis methodologies are more widely used, and as more smart devices from the Internet of Things (IoT) are attached to various smart grid components. Part of the risk assessment process will include determining the presence of data that can reveal information about individuals, throughout the smart grid.

Auditing should be included in the contract; without an audit requirement, a utility cannot validate that a CSP's assertions are in place and functioning as intended.

One requirement that is critical to address in the SLA is privacy[10] of energy customer data. Include how the CSP must address the privacy principles, such as those found in Fair

Information Practices Principles (FIPPs), the American Institute of Certified Public Accounts/Certified Internal Controls Auditor Generally Accepted Privacy Principles (AICPA/CICA GAPP), or the Organisation for Economic and Cooperative Development (OECD) Privacy Principles. These go beyond simple legal compliance; they are thoughtful critical assessments of privacy risks. Privacy regulations also vary between countries and between states. For this reason, the utility should know where the data will be stored in the cloud. One country may prohibit certain personal data from outside the country, while another country may allow external personal data.

While many of the types of data items accessible through the smart grid are not new, there is now the possibility that other parties, entities, or individuals will have access to those data items; and there are now many new uses for the collected data, which may raise substantial privacy concerns. More detailed energy usage data is also created through applications of smart grid technologies. As those data items become more specific and are made available to additional individuals, the complexity of the associated privacy issues increases as well.

Step 6: Identify Service Management Requirements

It is important to identify service management requirements. These include what should be monitored and reported (e.g., load performance, application performance), and what should be metered. These should also include how rapid provisioning should be (speed, testing, demand flexibility) and how resource change should be managed.

Step 7: Prepare for and Manage Service Failure

The final step is to prepare for and manage service failure, determining what remedies should be provided (e.g., service credits) and the associated liability limitations.
It is also important to understand how the disaster recovery plan will work, when needed.

Step 8: Understand the Disaster Recovery Plan

Disaster recovery is likely to be a joint effort between the utility and the CSP, and while many cloud SLAs promise 99%+ uptime, that is still four days/year of possible downtime, which few energy customers could tolerate. It may be possible to increase the uptime requirement, but the cost should be weighed against the benefit received.

Small- and medium-sized businesses often do not have the extensive disaster recovery processes that larger companies can afford, thus larger cloud providers may have more extensive processes that a smaller utility can benefit from. Both disaster prevention techniques, such as redundancy, hardening, and failover, should be addressed, as well as recovery from both natural and intentional disasters. The recovery plans need to be addressed in an SLA, but should be established from the utility's perspective beyond simply the CSP. The plan should define what a service outage is, how unexpected incidents will be handled, and what actions will be taken when service disruption is prolonged.

The risk mitigation will depend on the category or type of cloud services, as well as the specific business needs of the utility. It is important to understand that the risks and mitigations are different for SaaS, PaaS, and IaaS.

Step 9: Develop an Effective Management Process

The SLA should define appropriate status meetings, detailing attendance and reports to ensure compliance. An escalation process that is adequate to address the various types of business impact that are likely to occur should also be documented, along with a crisis management process for unanticipated issues.

Step 10: Understand the Exit Process

An SLA should also include an exit clause that details the exit process and the responsibilities of each party. Included should be what's involved in switching CSPs, either planned or as part of a disaster recovery process. Of primary importance is addressing the transmission and preservation of consumer data that is critical for the utility to maintain business continuity.

4 Conclusion

This paper describes the smart grid options for cloud services, and presents some examples of where the risks increase due to outsourcing part of the utility's business process to a cloud environment. One use of a cloud environment is for AMI processes, either initiated by a utility or even by an energy customer. In this case, how the energy customers' data is managed is of key importance, because customer data brings with it privacy issues.

The cybersecurity and privacy requirements documented in NISTIR 7628 are still applicable, and even when the risks are the same (between in-house and cloud implementation), the SLA should define when and how the CSP has the liability to repair and recover business functionality. It is important to include a specific auditing process, because without it, a service provider cannot be actively managed.

In addition to the advice contained in this paper and the referenced documents, another potentially useful guide is the recent *Procurement Language for Energy Delivery Systems*.[16] SLAs are written as part of the procurement process, along with the overall contract between a purchaser and a service provider.

5 Document References

1. NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011, Computer Security Division, Information Technology Laboratory, NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2. NIST SP 500-292, NIST Cloud Computing Reference Architecture, September 2011, Cloud Computing Program, Information Technology Laboratory, NIST, http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf.

3. *Practical Guide to Cloud Service Level Agreements*, Version 1.0, Cloud Standards Customer Council, http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf.

4. *Smart Grid: A Beginner's Guide*, http://www.nist.gov/smartgrid/beginnersguide.cfm.

5. NISTIR 7628, *Guidelines for Smart Grid Cybersecurity, Revision 1,* September 2014, available at http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

6. *Electric Sector Failure Scenarios and Impact Analyses*, September 2013, National Electric Sector Cybersecurity Organization Resource (NESCOR).

7. *Cybersecurity Procurement Language for Energy Delivery Systems*, Energy Sector Control Systems Working Group, April 2014.

8. NISTIR 7628, *Guidelines for Smart Grid Cybersecurity, Revision 1: Vol. 2, Privacy and the Smart Grid,* September 2014, Computer Security Division, Information Technology Laboratory, NIST, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=916068 .

9. *Cybersecurity Risk Management Process (RMP) Guideline*, May 2012, Department of Energy.

10. *NISTIR 7628 User's Guide - Smart Grid Cyber Security Implementation Guidelines*, available at http://sgip.org/NISTIR-7628-User-s-Guide---Smart-Grid-Cyber-Security-Implementation-Guidelines.

6 Contributors

- Avygdor Moise
- Bob Banks
- Elizabeth Sisley
- Leonard Chamberlin
- Leonard Jacobs
- Mike Swearingen
- Rebecca Herold and the SGCC Privacy Subgroup
- Scott Saunders
- Tanya Brewer
- William Hadala