The impact of cloud computing on the future of information technology cannot be overstated. In the mobile broadband enabled world, cloud computing increasingly provides the foundation of future services for consumers, enterprises, governments, and critical infrastructure. Therefore, ensuring the security and reliability of this pervasively developing paradigm is crucial for the economic viability our country and the safety of our citizens.

FCC TAC COMMUNICATIONS INFRASTRUCTURE SECURITY WORKING GROUP REPORT: CLOUD SECURITY ANALYSIS AND RECOMMENDATIONS

December 2013

TABLE OF CONTENTS

FCC TAC COMMUNICATIONS INFRASTRUCTURE SECURITY WORKING GROUP REPORT: CLOUD SECURITY ANALYSIS AND RECOMMENDATIONS

1. INTRODUCTION

This paper describes the Communications Infrastructure Security Working Group Group's analysis of cloud computing infrastructure security. This analysis defined the scope of the group's focus and identified areas of concern with security which established the foundation for the working group's recommendations to the FCC. The analysis and derived recommendations published here resulted from the working group's activities in the FCC 2013 TAC.

Scope and Objectives

In consultation with our FCC liaisons, the Communications Infrastructure Security Working Group clarified its scope to a focus on infrastructure security as it pertains to cloud computing and we adopted the following mission statement as put forth by the FCC.

> *The evolution of the nation's communications infrastructure towards a broadband IP-based network is occurring at an ever faster rate. This evolution includes an environment in which cloud based services are increasingly relied upon as substitutes for desktop applications, and even network services, and where attributes such as mobility, identity, and presence influence both the ability to access data as well as the context in which data may be presented.*
>
> - *In an emerging era where consumers and business rely upon cloud services for critical functions, what are the key areas of concern for security?*
> - *How cloud infrastructure and service providers best develop awareness of these issues and ensure that the ongoing evolution incorporates industry best practices, ensuring adequate protection for critical services?*

This mission statement led to the following key objectives for the work group:

- What are the top ten security concerns, and are there any "low hanging fruit" solutions?
- Who are the key cloud computing standards groups?
- What, if any, collaborative activities with industry, government, and academic organizations focus on cloud computing security?
- What is the security gap between what is needed and what is available or offered by cloud providers?
- What role could the FCC play in facilitating positive changes in the security of cloud computing market

Group Membership

FCC Liaisons:

Greg Intoccia
Ahmed Lahjouji

Members:

John Barnhill, GENBAND
Mark Bayliss, Visual Link Internet
Peter Bloom, General Atlantic
Peter Chronis, Earthlink
Adam Drobot OpenTechWorks (Vice Chair)
Dick Green, Liberty Global
John Howie, Cloud Security Alliance (Advisor)
Lynn Merrill, NTCA
Mike McNamara TWTelecom
S. Aon Mujtaba, Apple
Deven Parekh, Insight Partners
G. (Ramani) Pandurangan, XO Communications
George Popovich, Motorola Solutions
Jesse Russell, incNetworks
Paul Steinberg, Motorola Solutions (Chair)
Harold Teets, TWTelecom
David Tennenhouse, Microsoft
Donald Tighe, Verizon
Joe Wetzel, Earthlink

Approach

The group divided its analysis across the following three sub-working topics.

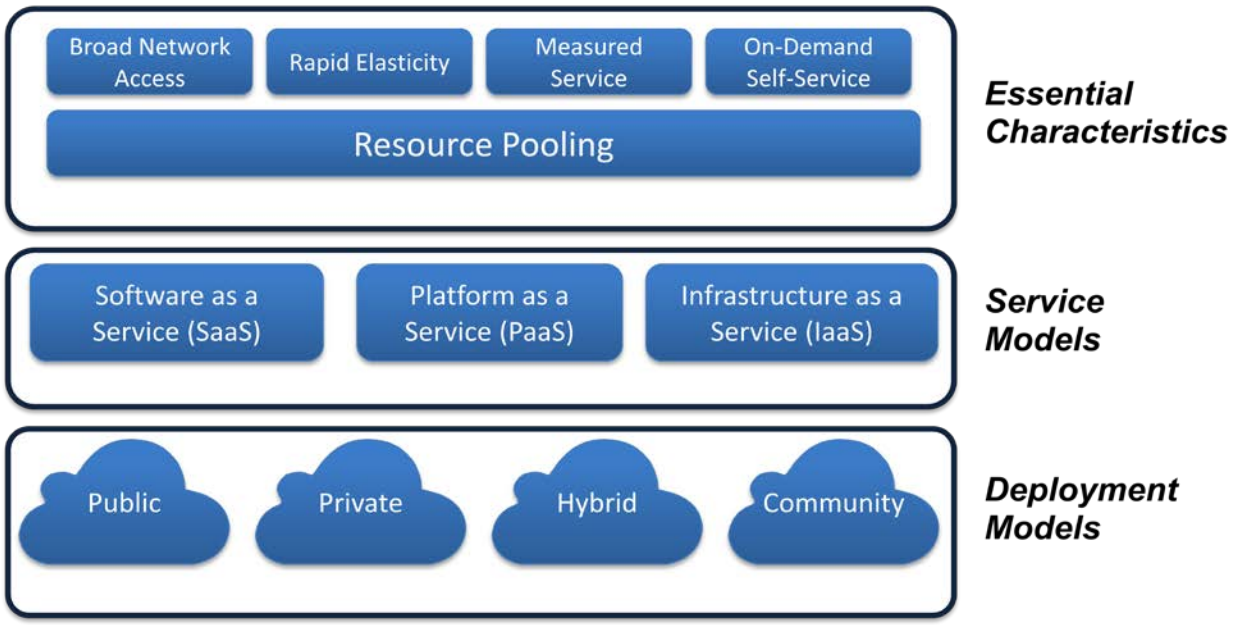
- Enterprise and Consumer Cloud Usage
- Critical Infrastructure (CI) and Mission Critical Cloud Usage
- Cloud Network Access

The first two topics relate to different user groups, applications and corresponding usage patterns that present substantially different deployment models and security considerations. The primary usage of cloud computing will be in support of consumer and economic services and applications and thus from an economic point of view this has an enormous implication to the future of the country. Critical Infrastructure and Mission Critical services will also increasingly find it desirable to employ cloud computing and these capabilities have obvious implications to the national security and economic viability of the country.

The third topic on cloud network access is necessary because cloud security for a complete use case is an 'end-to-end' proposition that also depends upon cloud network access reliability mechanisms as well as the application itself and their own security mechanisms. As organizations move more of their business requirements to the cloud for savings and efficiency purposes, it is important to focus on the network access for the particular type of cloud and the security implications for each. The network access types of the new perimeter should be considered from a security perspective for the new dynamics each provides. In addition, potential gaps of each method should be understood so additional security measures can be implemented and responsibilities understood between the customer, the Cloud Provider, as well as the Service Provider that provides the access.

2. CLOUD USAGE MODELS AND DEPLOYMENT SCENARIOS

The National Institute for Science and Technology has published definitions and characterization of cloud architectures in several excellent references.[1] [2] We have adopted this terminology wherever feasible and the following figure summarizes some of the major attributes and variants of cloud deployment models.



For purposes of this white paper, we are assuming that the definition of private clouds is from the perspective of the end points and where the assets physically reside. The population for private cloud applications is controlled through private (physical or virtual) access. The primary use of Private deployment is related to IaaS, and the secondary value contribution is PaaS.

Besides location of the physical assets, public cloud deployment is also distinguished from private cloud deployment in that public clouds mainly use the public internet for access but can also be defined as infrastructure that is accessed by multiple disparate parties. All of the issues around IaaS that exist for private cloud deployment exist in public cloud instances.

[1] "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, September 2011 (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)
[2] "Cloud Computing Synopsis and Recommendations," NIST Special Publication 800-146, May 2012 (http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf)

Contrary to what one might think, it is reported that today still approximately 90 percent of stored data is 'on premises' (stored privately) while only 10 percent is in public or shared clouds. That is obviously shifting rapidly but would point to the likelihood that a heterogeneous world will exist for some time. Some of the major Cloud Providers are emulating Private environments in Public spaces. The distinction between the Private and Public spaces is shrinking when virtualization of applications in any shared medium exists.

Our focus is on public, private, and hybrid clouds as well as network access methods to these (private line, [M]VPN, tunneling, Mobile Interface Devices, Internet Access (OTT)).

3. STATE OF THE INDUSTRY

General Technologies and Trends

The move of business applications to service oriented architectures has begun to drive service implementations that are well suited to cloud based solutions. WEB interface technologies such as HTML5, and REST based architectures have been key enablers for these architectural changes. There are also other key technologies pushing us to the cloud. For example, as noted by Gartner Consulting in their article "10 main strategic trends in IT in 2013", JavaScript performance will push HTML5 into the mainstream of application development for mobile devices. These technologies, in conjunction with the connected anywhere characteristic of the cloud and the growing number of tablet and mobile computing devices, are fast overtaking PCs as the primary devices to access applications. These began with email and instant messaging applications but has expanded greatly to include almost all facets of IT including as mobile commerce, finance, social networking, and management of personal/enterprise assets. The emergence of application stores enables a method to download business applications that cannot easily be displayed in a browser, again increasing the gravitation to cloud solutions.

With more people using mobile devices to access their personal content and services, it is only natural for them to want to use the same methods to access their business services as well. The cloud offers a cost effective alternative to in-house systems that can use TLS/SSL to encrypt traffic between clients and cloud based servers. Using TLS connections to services in the cloud removes the need for in-house solutions with a VPN connection to tunnel traffic between mobile devices and internal server. The cloud not only enables servers to be removed from the in-house server farm and placed in cheaper cloud based virtual environments, but also removes the need for any additional personnel and network hardware to support in-house VPNs, thus reducing the cost of the solution further.

The ease of use and availability of the cloud is also driving usage. Many vendors in the market today are offering free cloud storage up to a preset limit to farther entice individuals to start using cloud technologies. Individuals are using these services to share data and videos with their friends as well as backup home computers. For a nominal fee, cloud providers will increase the storage capacities of these services to the end customer. As these services are becoming more popular, small business are quickly beginning to realize the low cost of these services and take advantage of the cloud for data backup and other software services. Using software services offered by clouds small business can now quickly implement business solutions that might otherwise be outside their budget or technical knowledge to implement. The reduced cost of cloud computing is also enabling small businesses to reinvest in product development and innovation, as noted by WordPress in their article "Push for cloud adoption brings savings for SMEs". This has not gone unnoticed by bigger businesses.

In an effort to make their businesses more agile and to reduce cost, mid-sized to large companies see the cloud as a way to cut cost and improve profit or lower prices to their customers. A big plus for the larger business moving to the cloud is reduced time to implement a service. Lead times for purchase orders, procurement and setup are significantly reduced when using the on-demand nature of the cloud. Using the cloud, virtual servers can be created in minutes where it could have taken weeks to obtain and setup physical devices on premise, making big business more "agile". In short, not only technology but today's economic climate is pushing all types of businesses to consider cloud based solutions that would never have considered using a hosted service in the past. Government, Public Utility and Public Safety entities are not immune to these forces.

Though moving to the cloud offers economical alternatives for some applications, moving to the cloud is not without its risks. Security threats must be considered when moving applications from closed in-house systems to public accessible clouds. The Cloud Security Alliance (CSA) is a not-for-profit industry forum specifically focusing around the issues of cloud security and its implications for adoption and promulgation of cloud computing. The CSA has recently published its assessment of the top threats to cloud computing – the so called 'Notorious Nine.'[3]

- Data Breach
- Data Loss
- Account Hijacking
- Insecure APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Issues

The CSA indicates that the top threats to (established) cloud computing environments are different than those perceived relative to those considering adoption of cloud computing.

There is an enormous amount of activity in government and industry addressing aspects of cloud security that could be consulted and/or collaborated with for future activities. Appendices 1-3 of this document list organizations that were identified during our analysis as having some stated activity or intent relative to cloud security:

- Appendix 1: Current Industry/Government Initiatives to Address Gaps
- Appendix 2: Government/Industry/Standards Organizations Active with Cloud Security
- Appendix 3: Mission Critical and Critical Infrastructure Security and Privacy Issues from NIST 800-144

The importance of this topic is perhaps best underscored by the focus and importance that the EU ascribing to this area. The European Network and Information Security Agency (ENISA) has published an analysis commissioned by EU member states that clearly points to the view the cloud computing is critical infrastructure in and of itself.[4]

Enterprise and Consumer Cloud Usage

[3] "The Notorious Nine – Cloud Computing Top Threats in 2013," Cloud Security Alliance, March-2013 (https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013)
[4] "Critical Cloud Computing – A CIIP Perspective on Cloud Computing Services," European Network and Information Security Agency (ENISA), Version 1.0, December 2012.

Consumer

Convenience has driven consumer adoption of cloud services which offer unfettered access to data and services from anywhere a network connection is available. Search portal, social networking and online shopping sites are among the most popular consumer cloud services today.[5] Online banking, travel, healthcare, cloud file storage/backup and email services are also popular.

Many cloud services collect significant amounts of data directly or indirectly as a result of the consumer's use. Some of this information is considered either sensitive, protected by federal/state law or governed by the provider's privacy policy. The most sensitive information can be used to directly establish a user's identity (ex. social security number, biometric records) or can be indirectly associated to an individual (ex. medical, financial records).[6] In many cases, the consumer doesn't really know much about the security and policies of cloud providers entrusted with their data. Privacy group EPIC highlights the implications of heavy cloud usage by consumers stating:

> "…when users place their data and applications on centralized servers, they lose the ability to maintain complete control of that information…" adding "…one of the biggest risks of storing data in the cloud is the possibility that this data will be accessed by unwanted third parties."[7]

In 2013 alone, account details, files, credentials and/or billing information belonging to over 100 million file sharing, social networking and online shopping cloud service users were illegally accessed via data breaches.[8]

Further, consumer cloud users have concerns about how their personal cloud usage habits are recorded and used to market products and services to them. The Federal Trade Commission has taken action over the last few years to force companies to alter privacy and security programs to either align with privacy best practice principles or force companies to deliver on privacy commitments made to customers.[9]

Complicating matters further, many popular consumer cloud services are built on top of cloud services platforms delivered by a third party. Securing systems and platforms becomes more complicated in hybrid cloud models where the tenant (consumer cloud services provider) and the platform provider (enterprise grade cloud services provider) share responsibility for securing sensitive consumer data.

In all cloud deployment scenarios it is important to understand the responsibility and accountability that each party has for the various pieces of the end to end security functions. In the past, it was safe to assume that in nearly all cases, the entity with direct relationship with the consumer had the primary responsibility for security and privacy of data placed in its care even if it partnered with a cloud provider to deliver services to the customers. That may be changing. This year, the US Department of Health and Human Services issued guidance to providers delivering IT services (aka Business Associates) to healthcare providers. Starting in 2013, Business Associates will

[5] "Top Global Sites, " Alexa, November 12, 2013, (http://www.alexa.com/topsites/global;1)
[6] "Guide to Protecting the Confidentiality of PII", NIST, April 2010, (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf)
[7] "Cloud Computing Privacy", Epic, (http://epic.org/privacy/cloudcomputing/)
[8] "Hack Exposes Data", NY Times, April 26, 2013 (http://bits.blogs.nytimes.com/2013/04/26/living-social-hack-exposes-data-for-50-million-customers/?_r=0)
[9] "Making Sure Companies Keep their Privacy Promise to Consumers," FTC, (http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml)

also be subject to fines if they directly contribute to unauthorized disclosures of patient health records.[10]

Enterprise

Enterprises of all sizes have struggled with supporting the explosive growth and cost associated with supporting infrastructure and customer and commercial applications. Looking for ways to reduce fixed capital costs, many companies have moved or migrated to enterprise cloud applications. Industry expert Gartner has predicted that by 2016 "cloud computing will make up the bulk of new IT spend."[11] Gartner continues that SaaS and IaaS spending by enterprises will grow by more than 30% annually in some markets.

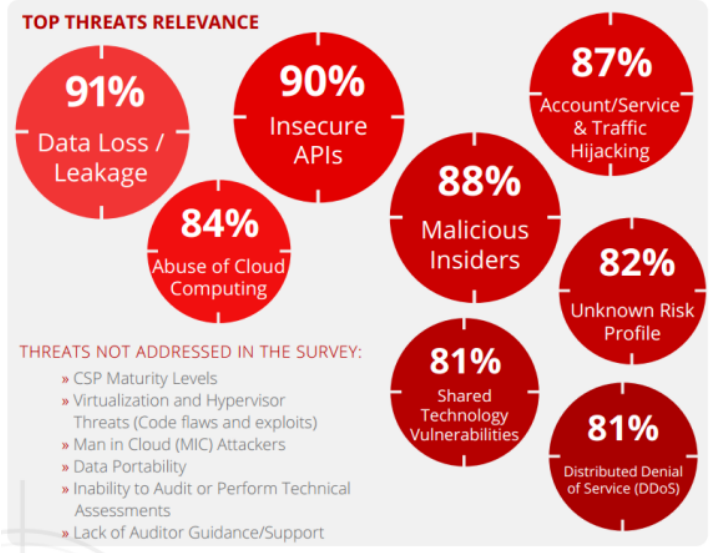
As enterprises move more applications and services to the cloud, they also are moving more of their enterprise and customer data. The challenge most enterprises face when moving applications and services to the cloud is defining confidentiality, integrity and availability (aka CIA) requirements and evaluating whether cloud providers can satisfy their needs. Public, private and hybrid cloud models have all evolved based on a landscape of different enterprise level requirements that are often driven by CIA requirements. As enterprises move to the cloud, they often struggle to evaluate and track their cloud provider's ability to deliver and meet CIA. Many enterprises migrate applications to public or private cloud solutions without fully understanding how the cloud provider will help them deliver and protect their applications.

SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Cloud Service Security Responsibility Model

As the figure above demonstrates, responsibility for the operation and efficacy of technology services delivered as part of cloud service types vary. In a typical SaaS cloud services model, the provider has a greater role in delivering security across all elements of the service than in most typical IaaS models.[12] Enterprises need to be thoughtful and considerate when moving applications to the cloud to ensure they address areas where they continue to have partial or total responsibility for managing risk.

[10] "New Rule Protects Patient Privacy, Secures Health Information," Department of Health and Human Services, January 2013 (http://www.hhs.gov/news/press/2013pres/01/20130117b.html)
[11] "Cloud Computing will Be Bulk of IT Spend", Gartner, October 24, 2013 (http://www.gartner.com/newsroom/id/2613015)
[12] "GRC Stack Training", Cloud Security Alliance, June 2011, (https://downloads.cloudsecurityalliance.org/ initiatives/grc /CSA_GRC_Stack_Training-2011-03-06.pdf)



Top Cloud Security Threats

Industry Consensus Top Cloud Threats above identifies critical areas of risk the CSA's most recent threat survey of enterprise cloud users. [13] In the survey, enterprise cloud customers identified a number of key security issues they believe drive risk to confidentiality, integrity and availability. Although some of these risks are no different than if the enterprise customer chose not to host infrastructure or applications in the cloud, some risks are unique or potentially elevated as applications and infrastructure are moved to the cloud. Assessing CIA risk becomes a unique and interesting challenge as enterprises evaluate and move applications to the cloud. Ideally, enterprises need efficient ways to evaluate a cloud service provider's security controls structure and determine whether or not they are effective. Certification and audit options designed to help enterprises evaluate cloud providers control environments can deliver are key to success and will be explored in detail later in this document.

Critical Infrastructure (CI) and Mission Critical Cloud Usage

The definition of 'Critical Infrastructure' is not universally agreed upon across the industry; however, for purposes of this paper, we assume the definition set forth by the U.S.A Patriot Act of 2001.[14]

> ***42 USC § 5195c*** *(e)* ***Critical infrastructure defined***
> *…**"critical infrastructure"** means **systems** and **assets**(and **networks**), whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a **debilitating impact** on security, national economic security, national public health or safety, or any combination of those matters.*

[13] "The Notorious Nine: Cloud Computing Threats in 2013", Cloud Security Alliance, February 2013 (https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf)
[14] U.S.A. Patriot Act of 2001, Public Law 107-56 (42 U.S.C. 5195c(e)), Section 1016(e)

*Critical infrastructure is the backbone of our nation's economy, security and health. We know it as the **power** we use in our homes, the **water** we drink, the **transportation** that moves us, and the **comm. systems** we rely on to stay in touch with friends and family.*

CIJS DATA IN CLOUD

For Mission Critical applications, one particular concern with migrating to the cloud is related to restrictions around certain data stored within these applications. One example of this data is Criminal Justice Information (CJI). CJI is subject to rules that restrict access by law. Police officers accessing this data can determine if an individual has any outstanding warrants that might give the officer reason to detain the individual, or to use extreme caution when approaching a vehicle during a routine traffic stop. Other CJI includes criminal histories of the general populous, driver's license data and basically any other information needed by criminal justice officers and employees to carry out daily tasks.

The Federal Bureau of Investigations' Criminal Justice Information Services (CJIS) Division was established in February 1992 to serve as the focal point to create a single centralize repository for criminal justice information in the FBI. It merged the handling of all data related to the criminal justice system under one division of the government. With the creation of this repository of data, restrictions were put in place on any access by a computing device.

Since CIJS data stored on a computing device is subject to laws that restrict the access to the data, many concerns have been expressed by municipalities as to the ability of a cloud provider to meet the strict controls required to store and access this data. The FBI Information Security Office generated a paper in 2012, titled "Recommendations for Implementation of Cloud Computing Solutions", with recommendations for any CIJS community member implementing cloud based computer solutions that access CJIS data. This paper outlined the technical and operational issues impacting the use of clouds with CJIS data. The areas examined were:

- Transmission of Data
- Storage of Data
- Application Access and Service Layering
- Emergency Access and Disaster Recovery
- Retention and Backup
- Legal
- Access Authorization, Authentication methods, and Identity Management
- Service Provider Viability and Structure
- Audit and Monitoring Capabilities and Authorization
- Cryptographic Key and Certificate Management

Use cases discussed later in this paper for Mission Critical and CI must take into consideration the recommendations of this report to assure that the end-to-end security and accountability of data access does not prevent the use case from being realized via a cloud based solution. Though CI data is not subject to the same laws as CJIS data, the same due diligence is warranted when evaluating security risks with respect to the aforementioned list to assure attacks against the CI systems are prevented wherever possible.

Cloud trends specific to Government and Public Safety

Government and Public Safety entities worldwide have begun to realize the potential offered by using cloud services in day to day business needs. This is being driven by both cost reduction needs and a time-frame alignment of Government computer usage with elasticity and connected everywhere characteristics offered by the cloud. The US government has published the following characteristics about its computer usage, which by chance or design align well with offerings in a cloud base service solution. These characteristics are pulled from the 2011 DHS report, "Federal Cloud Computing Strategy":

- low asset utilization
- a fragmented demand for resources
- duplicative systems
- environments which are difficult to manage
- long procurement lead times

Cost reduction and these characteristics to government computer usage led Vivek Kundra (at the time U.S. Chief Information Officer) to recommend instituting a "Cloud First" policy when designing computing solutions for government agencies. On December 9, 2010; the Office of Management and Budget (OMB) released the "25 Point Implementation Plan To Reform Federal Information Technology Management", officially establishing the Cloud First policy and requiring agencies to use cloud-based solutions whenever feasible for any given computer service. Since that mandate, other initiatives have begun to drive the government toward cloud usage. Following the mandate, all agencies were to re-evaluate their computer sourcing strategy to include consideration and application of cloud solutions as a part of their budgetary process. These characteristics and views are not unique to the US government.

To further U.S. Government adoption of cloud technologies, On December 8, 2011, the Security Authorization of Information Systems in Cloud Computing Environments memorandum (FedRAMP Policy Memo) was issued by the Office of Management and Budget. This memorandum established the Federal Risk and Authorization Management Program (FedRAMP) to provide processes and procedures to help government agencies assess and design cloud solutions for their needs. The purpose of the initiative around FedRAMP, which is taken from their CONOPS, is to:

- Ensure that cloud based services have adequate information security
- Eliminate duplication of effort and reduce risk management costs
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies

Given that U.S. mandates are pushing agencies to the cloud and federal law controls access to criminal justice information, both FedRAMP and CJIS considerations will need to be taken into account when identifying areas of concern in cloud solutions for Mission Critical and Critical Infrastructure use cases.

There are many instances where the government has already moved to cloud based services for business activities. The following are data points to support this fact.

- The Interior Department was the first agency to move records to the cloud with its eERDMS implementation (Interior takes records management to the cloud)

- The success of records management in the state of Oregon has led them to start a program to implement it state-wide (Oregon rides cloud to statewide records management system).
- The Chicago Department of Innovation & Technology (DoIT) recently started migrating their email and other desktop applications to the Microsoft 365 cloud service (Chicago moving 30,000 employees' e-mail to Microsoft cloud).
- All software for the 2012 Democratic presidential campaign was hosted on Amazon's cloud (How a 2012 Presidential Campaign Ran on Amazon's Cloud).
- The city of Panama Florida is using Google SaaS core applications to run day to day operations (Panama City promotes open government with Google Apps). According to CNG in (Fla. city takes secure path to Google cloud) they a have also added a layer of security to the Google cloud.

The "Cloud First" mandate has accelerated the use of clouds in areas where it seemed to be the most risky to use. We are even starting to see the use of cloud technologies spilling over into mission critical applications such as Computer Aided Dispatch (CAD) and 911 systems. As the government relies more heavily on public cloud solutions in this space, the need for assurances that the system is secure has never been greater. Questions still arise as to the ability of clouds owned by third parties to meet data privacy and security needs by some Critical Infrastructure and Mission Critical applications within the government.

An alternate approach to moving services to a public cloud can be taken. Both open source solutions and vendor appliances offer cloud platforms that enable the creation of internal private clouds. Internally hosted clouds may be the only practical solutions in the most restrictive application implementations with respect to security. An internally hosted private cloud will offer the security needed for applications with strict security requirements but will not offer the economy of scale offered by the public cloud providers. An approach that may address needs for strict data control and benefit from a level of economy of scale is a community (owned) cloud. Community clouds will address issues such as data location and offer more controls over the data, as compared to public clouds solutions.

Cloud Network Access

Seeing faster adoption of hosting and outsourcing application environments to cloud infrastructure providers.

- Largely driven by the cost savings (typically capital and labor) that outsourcing is bringing to CIOs

Security is still one of the largest concerns by users of cloud infrastructure – however it is also the greatest areas of improvement

- Strong sentiment of "cloud providers MUST know more than I do about protecting my data"
- Cloud Providers are looking to more to fill open server capacity rather than protecting users' data. Their model is to "let everyone in"
- The Service Provider must protect MY data as I access the Cloud Service Provider

Various security methods are used when considering network access to outsourced applications utilizing cloud infrastructure

- Private Line / Dedicated Transport – one of the most secure methods but also one of the most costly to an enterprise's business
- Virtual Private Network: offers decent security protection when coupled with encryption methodologies such as SSL (Secure Socket Layer)

- Internet Access: least secure method of protecting data and least desirable when needing to track down and troubleshoot performance issues and IPSec (also referred to as OTT – Over The Top)

No clear ownership of who is ultimately accountable – should be whoever owns the customer relationship

4. USE CASES

Enterprise and Consumer Cloud Use Cases

There are quite a few possible use cases to consider. For purposes here we are describing what we consider to be the most common uses of cloud environments that yield issues that are generally applicable to all cloud deployments.

Use Case 1: Consumer SaaS Cloud

In a consumer (aka consumer to business) SaaS model, the cloud provider would be responsible for nearly all elements of security. Consider the case of a cloud file collaboration service. Nearly all layers of the service (data, application, compute, storage, network and physical layers) are the responsibility of the cloud provider. Consumers may have some limited responsibility to protect authentication credentials or perhaps to limit direct access to file synch software (i.e. similar to synch software used by iCloud, Box, DropBox). Consumers may unintentionally disclose credentials if a malicious programs on their computer record browsing behavior and log keystrokes when they access the cloud storage service.

In consumer cloud models, privacy is an important element of the service. The AICPA's privacy guidance suggests that providers clearly define in writing how they plan to collect, use, retain and dispose any personal identifiable information collected in the delivery of the service. Privacy commitments made to the customers must be operationally followed (for example limits on the type of personal data that is collected) by the provider. The Federal Trade Commission has fined providers who do not deliver on privacy commitments made to consumers or who failed to protect customer privacy.

Use Case 2: Enterprise SaaS Cloud Model

The use of public cloud hosting products by large and enterprises is on the rise. In this service model, cloud service providers deliver virtual machines used by enterprises to deploy public and private applications. In this model, the provider is responsible for delivering physical and logical security for compute, storage, and network. Depending on the delivery model, it is possible for the provider and enterprise consumer to share responsibility at the application and data layers. Often, cloud service providers only deliver limited application layer functionality for example: some deliver fully provisioned guest operating system (patching, anti-virus, etc.), some deliver guest operating systems and additional services like database support; others deliver only virtual machine access (enterprises are responsible for configuring and deploying the guest cloud system). In all three models described, there is shared enterprise/provider responsibility for securing application and data layers.

Enterprises should be careful as they move applications into the cloud to ensure they clearly understand what services the provider is responsible for delivering. Many providers deliver services in tiers, security monitoring,

general operations support are often offered as value added services or within service tiers often delivered for additional cost. Most providers also offer SLAs that govern service availability. Improper due diligence could result in security or availability gaps that fall short of the enterprise's needs.

Use Case 3: Enterprise IaaS Cloud Model

In a classic collocation infrastructure as a service model, service providers are often responsible for delivering physical space, commercial electric power and network access (either directly or indirectly). An enterprise would host their physical servers in a rack or cage provided by the service provider. Physical security is often the primary responsibility of the provider. SLAs commitments are often made for commercial power and facilities access (including emergency access procedures). In a typical collocation model, logical security for storage, compute, application and data layers is the responsibility of the enterprise consumer. Often, some shared network security responsibilities exist if the collocation provider is responsible for delivering or enabling network access.

Critical Infrastructure and Mission Critical Cloud Use Cases

This section explores the most relevant cloud based use cases within the mission critical and critical infrastructure vertical space. A more detailed exploration of the uses cases can be found in the accompanying document titled, ***"Expanded findings Around Mission Critical and Critical Infrastructure Cloud Usage: A More In-Depth look at the Relevant Use Cases and Areas of Concern"***.

Point Solutions

Business critical applications such as aging revenue collections systems used by government are replaced by a cloud based shared revenue collection system between county, city and state. In this use case the loss of or compromise of the revenue system would negatively impact the government's ability to collect needed income and expose private information about citizens that could be used to steal ones identity. Municipalities such as Cook County IL have announced plans to make transitions to cloud based systems over the next few years. Their plan can be viewed at
http://legacy.cookcountygov.com/secretary/committees/Finance/FY2013/budget%202013/Technology%20budget%20presentation%20-%20FINAL.pdf

Business Intelligence Applications and the use of CJIS Data

Business Intelligence applications used by public safety to process records and manage data are hosted in the cloud to reduce cost of the system. The applications may be required to handle CJIS data. Cloud providers would not only need to meet access requirements such as two factor authentication, but also the personnel that maintain the system would need to be vetted against CIJS requirements. Restrictions on data location will also need to be addressed by any cloud implementation for this use case. The city of Panama Florida's solutions using SaaS from Google (mentioned earlier) is an example of this.

Instant message and Email services are being hosted in the cloud. After seeing the highly publicized failure of LAPD trying to move their system to the cloud, we must consider the impact of exposing this use case to CJIS data. The system must also be capable of protecting CJIS data in the case that the data is sent to an outsider with proper clearance, such as in an email attachment.

Real-time data applications that provide 911 operators and first responders with secure access to critical information are being hosted in the cloud to reduce the cost of the system. In this scenario, data for each agency and department must be segregated by municipality and access must be restricted to designated roles within each municipality. High availability requirements must be met to ensure this information is available to first responders at locations of any incident.

Data Analytics

Data set sizes used in data analytics will prove to be too large and costly to own and operate by individual government agencies. There are already instances of the government using clouds to create large data stores. As reported by Tech Crunch, the National Security Agency is pursuing its interest in united data archives by taking its information into a cloud environment. Attunity also reports the NSA has moved away from silos of data owned by each division in favor of a central cloud base repository in their article "Government project serves as cloud data storage example"

Radio System Bridging

Software solutions to patch disparate radios systems together will use Software–as-a-Service to link the radio systems using the cloud. In this use case the bridging server would run in the cloud. System to system interfaces would be exposed to the cloud by the radio the systems to enable the connection. The solution will allow fire, police, emergency management and other agencies to connect their private push to talk systems in response to a situation that requires the coordination or monitoring of communications across multiple municipalities. The following article outlines this use case http://fcw.com/articles/2009/04/16/cloud-computing-moving-into-public-safety-realm.aspx.

CI: Consolidation into a single user experience

Within geographic regions (e.g. cities, municipalities) there exists disparate systems with widely varying user interfaces. However these entities all have similar critical infrastructures to maintain, such as sewer, water, power, fire & rescue, and police. Moving to a cloud environment enables various entities to consolidate their resources and provide their users with a common user experience, enhanced functionality, and still maintain their dissimilar back-end systems. One challenge to providing a single interface is authentication and authorization across several sets of legacy systems that have different login methodologies.

CI: Process Monitoring

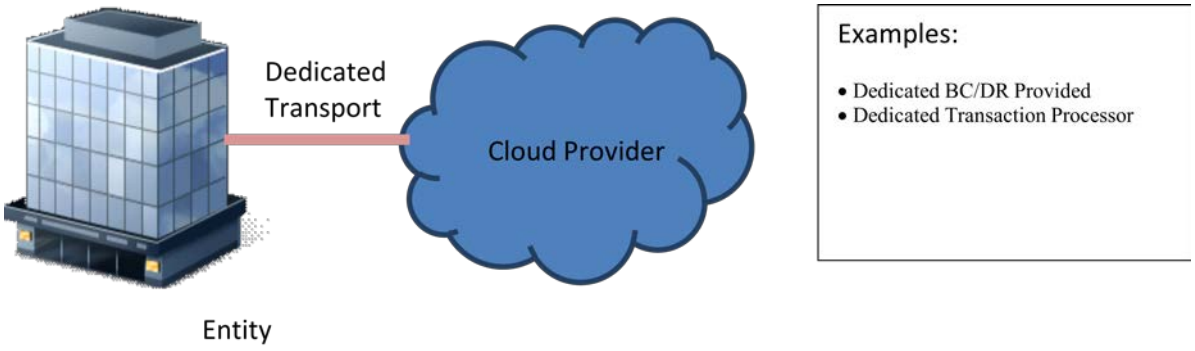
Several instances of Critical Infrastructure (e.g. SCADA) have process monitoring as a core function. Water, power, and sewage systems all have large sensor networks for monitoring industrial control systems (ICS) environments. By using the cloud as a repository for information and for processing sensor data, operators and engineers can receive analytical information while they are on the move outside the conventional control room on tablets, smartphones, and other portable devices. Migrating SCADA devices to the cloud permits access from any Internet-connected location, allowing easy access to data. Moving to the cloud also enables scalability and can establish baselines for redundancy and uptime while lowering costs. For example the article, "Cloud-Based SCADA Offers Alternatives to Traditional Systems" in Waterworld magazine talks about the cost effectiveness of moving SCADA water and wastewater treatment plants, and this article in InTech magazine provides several examples of HMI/SCADA solutions hosted in the cloud that provide remote access, any time, any place.

Cloud Network Access Use Cases

As organizations move more of their business requirements to the cloud for savings and efficiency purposes, it is important to focus on the network access for the particular type of cloud and the security implications for each. The network access types of the new perimeter should be considered from a security perspective for the new dynamics each provides. In addition, potential gaps of each method should be understood so additional security measures can be implemented and responsibilities understood between the customer and the Cloud provider, as well as the Service Provider that provides the access as the link between the two. Below is list of common models:

Private Network Access

Use Case #1 – In this model, access to the cloud is private via dedicated transport between two entities.



Issues – This option offers the greatest security.

- Cost – Greatest cost requiring full-time dedicated access.
- Encryption – If required to protect against physical threats.
- Business Continuity/Disaster Recovery – BC/DR considerations for this case increases cost.

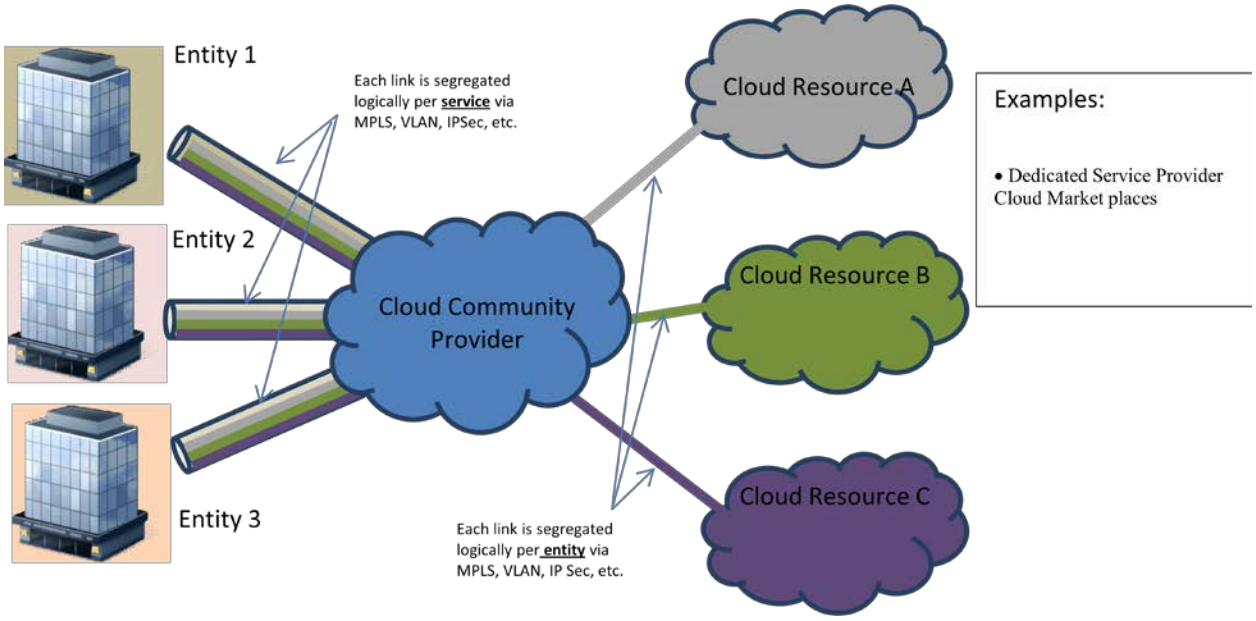
Concerns/Future Development-

- Perimeter protection – Access between the entities should be limited to only the type of traffic required – controls should be established to filter and manage the data. Defense in depth scenarios are considered here as this link can be considered a part of each other's DMZ (Demilitarized Zones).
    - Defense in Depth is an information assurance concept in which multiple layers of security controls are placed throughout an IT system. The intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedures, technical and physical for the duration of the system's life cycle.[15]
- Data Considerations – Data protection must be managed between the two entities.
- DDoS is less of a concern in this model

[15] *Wikipedia: http://en.wikipedia.org/wiki/Defense_in_depth_(computing)*

Community/Hybrid Network Access

Use Case #2 - In this model, dedicated network resources are shared amongst a small group of private entities.



Issues – This model provides security based on the fact that it's a closed model. This model assumes dedicated resources.

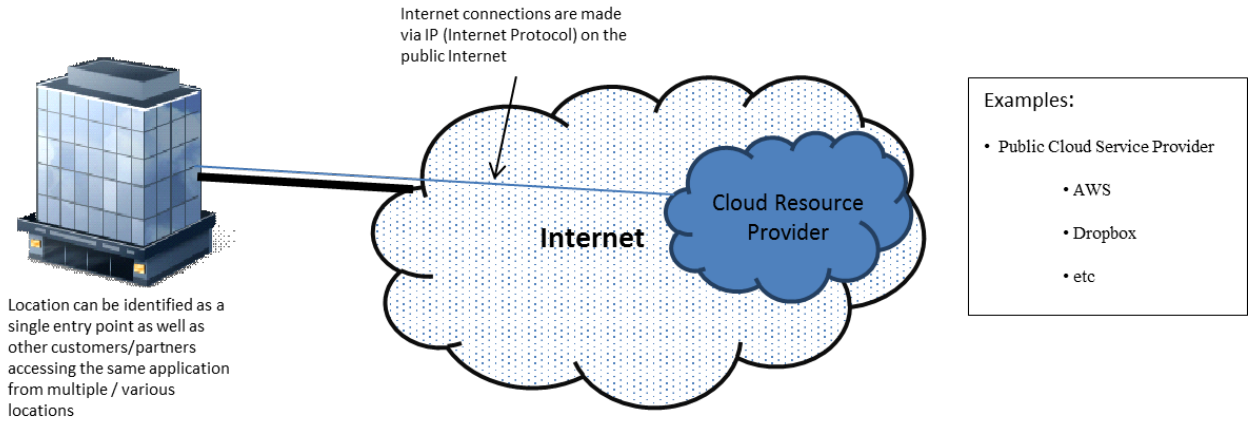
- Cost – This option realizes cost savings by leveraging links used to provide converged cloud solution across a single link.
- Encryption – Required where network segregation does not satisfy regulations. Encryption between the Cloud Resource provider and the entity would insure confidentiality from the Cloud Community Provider.
- Business Continuity/Disaster Recovery – BC/DR can be provided via the Cloud Community Provider.

Concerns/Future Development

- Perimeter Protection – Defense in depth must be adhered to at each logical segregation point, which should each be considered a separate security zone. Care also is required at the cloud community provider and cloud resource provider as they provide areas of exposure. Authentication, Authorization and Account is considered here.
- Data Considerations- Data protection is considered at both the Cloud Community Provider and the Cloud Resource Provider.
- DDoS can be a concern in this model if any point serves has exposure to the Internet

Public Network Access

Use Case #3 – This model has the most exposure with regards to security. Everything is accessible by the public Internet.



Issues – This option has the most exposure…and it certainly the widest utilized to access the Cloud

- Cost – This option has the most savings as it leverages the internet and has no dedicated facilities.
- Encryption – This is highly recommended. Sensitivity to integrity and confidentiality is required as all traffic is over the public Internet. Considerations should be made for both data in motion and data at rest.
- Business Continuity/Disaster Recovery – BC/DR can be provided via the Cloud Community Provider.
- Perimeter Protection – Defense in depth required. Restrictions must be applied to prevent malicious activity.
    - Options – Firewall, IPS, WAF, DDoS Protection, etc
- Supporting Infrastructure Protection – Protection of supporting infrastructure exposed to the Internet is a must.
    - Option – DNS, BGP, etc
- Data Considerations- Data will be co-mingled at the Cloud Resource Provider. Considerations as to what kinds of data can be applied to certain types of data being exposed to the cloud.
- DDoS becomes a concern in this model. Every point in this model subject to an Internet attack.

Concerns/Future Development

- This model is most often used to provide access to mobile devices. Greater consideration is required to prevent additional mobile functionality from being used as a pivot points by hackers.
- Security is provided by the application is this case. Secure Coding practices should be followed to insure vulnerability cannot be exploited to gain access or data.

- Based on the Untrusted nature of the Internet consideration should be given to the many different attack vectors such as:
    - MiTM(Man in the Middle) - Where communication is intercepted
    - Session Hacking – Where a valid communication session is exploited.
    - Authentication Based Attacks – Where authentication is manipulated.
    - Unvalidated redirects and forwards – Where victims get falsely redirected.
    - etc

5. IDENTIFIED AREAS OF CONCERN

Consumer and Enterprise Cloud Findings

Not all service providers possess the same level of IT security proficiency. This creates problems for uneducated enterprises and consumers who are unable to evaluate security proficiency when making purchasing decisions. While there is a lot of literature available that outlines best practices in cloud security, it is temporal in nature and it requires an investment from the enterprise/consumer to learn about it. There are no central, adopted best practices defined for evaluating security in the cloud therefore no standard mechanism for auditing and certifying a service provider's network and application security in the cloud.

A central certification/audit scheme of standards and best practices must be developed and widely adopted by both consumer and enterprise cloud providers designed to help evaluate security, privacy, integrity, availability and confidentiality of cloud services.

Data security is often the responsibility of the enterprise consumer in certain cloud model (IAAS, some SAAS applications). Since IAAS, PAAS and SAAS enterprise applications are often built on top of a provider's cloud stack, any certifications scheme would be incomplete if it stopped at the hypervisor or operating system layer. Any security or privacy certification scheme must account for hybrid cloud models where security is a shared responsibility. For example, encryption is really an enterprise responsibility, while separation of the data bytes is a cloud function, and which applications have access to the data is really and enterprise function.

Many quality third party assessment services are too expensive for many small and medium sized businesses to afford. Public and private industries must collaborate to promote private sector innovation designed to deliver quality, repeatable and reliable security testing aligned to a central standard that is cost effective for small and medium enterprises to adopt and use.

Critical Infrastructure and Mission Critical Cloud Findings

This section looks at some concerns that arise when planning to move mission critical and critical infrastructure services to the cloud. For this section, we scanned industry trade journals and technology forums. We also interviewed subject matter experts in cloud and hosting technologies. This section takes a look at topics that have bubbled to the surface during our analysis.

For additional information beyond what is described in this section, please refer to the supporting Working Group document titled, ***"Expanded findings Around Mission Critical and Critical Infrastructure Cloud Usage: A More In-Depth look at the Relevant Use Cases and Areas of Concern"***. This expanded document describes several areas of concern that were examined at a high level by the Working Group, but did not directly link to the selected short list of recommendations to the FCC. The reader should nevertheless find this expanded paper useful in understanding the breadth of work taken on by the Working Group.

Identified areas of concern:

a. SLA contract language
b. Identity management
c. Education
d. Cloud certification programs

SLA CONTRACT LANGUAGE

A key to understanding a cloud service provider's (CSP)'s policies with respect to security, data privacy and data integrity should be the terms and conditions of the CSP's SLA with the customer. Building expectations both on the CSP and customer sides and successfully executing on those expectations is a benchmark for a good SLA. But how good are the SLAs today? Are federal agencies and utility companies with no cloud experience equipped to evaluate a CSP's SLA to ensure that privacy, security and integrity needs are met by the offering?

What are the real issues with SLAs? Some shortfalls in SLA's include; a lack of "what if" scenarios as reported in Cloud computing SLA failures: Preparing for the aftermath by Search Cloud Provider, vendors not meeting expectation such as reported in the article Mimecast server goes down, putting 100% SLA in tatters, and the inability to start sleeping VMs combined with dependent service failures. Given the number of instances reported in the media of cloud services not meeting expectations, there seems to be a substantial gap related to customers' understanding of what is and is not covered in SLAs. Mission Critical and Critical Infrastructure clouds will be even more demanding on cloud providers.

There have been some guides created over the last few years that can be used to address this gap. Below are listed examples of these guides:

- The Cloud Standards Customer Council (CSCC) has developed and published a document called the Practical Guide to Service Level Agreements (SLA).
- Standard clause templates published by FedRAMP Standard Contract Clauses.
- CSA's SLA Working Group, which published SLA Guidance document

Of these guides, the most appropriate for MC and CI services would be the FedRAMP template containing Standard Contract Clauses to cover federal agency cloud implementations. However, there is the question whether the standard agreement clauses listed in the FedRAMP template cover enough detail, especially in light of some of the failures pointed out earlier. For instance, the standard template does not mention availability of services or ability to expand the service to meet on-demand needs. Availability is mentioned in the Contingency Plan Template but this speaks to the recoverability of a service. In addition, the scope of FedRAMP is federal agencies. Who do state and local agencies turn to for guidance? Is it appropriate to have them use FedRAMP as guidance?

Other areas that could be added to the template are statements for classified data, meeting CJIS requirements, and statements that place expectations on cloud vendors for the location of administrators and other IT support personnel. Even with the lack of items in standard clauses that are mentioned here, the Standard Contract Clauses template from FedRAMP is a good place to start. **To summarize: SLA guidance needs to be developed that addresses the previous topics discussed in a template that can be used across federal, local and state public safety entities for Mission Critical Systems.**

IDENTITY MANAGEMENT

The biggest needs for Identity and Access Management (IAM) in the cloud that are not adequately being met today center around Trust Frameworks, Attribute Exchange, and Provisioning. Authentication technologies such as SAML and OpenID Connect are well understood and are seeing increased rates in adoption, as are API authorization technologies such as OAuth, which protect RESTful communications.

Trust Frameworks address not only the technology aspect of IAM but also the policy, governance, and legal aspects of IAM. One of the most challenging aspects of Trust Frameworks entails Identity Proofing and the required accreditation of Identity Providers when higher levels of Identity assurance are required. Current efforts in this area have been less than efficient and lack scalability. In general, Trust Frameworks and large-scale federations have seen limited success and more work in this area is required.

A second area that will present a challenge will be the subject of attribute exchange. Clouds will be required to obtain attributes from a variety of attribute providers in order to make fine grained authorization decisions, and clouds may also be called upon to expose attributes to other clouds. This is an immature area that is beginning to see more work around it.

The third area that will present a challenge will be the subject of provisioning enterprise roles within the cloud providers. Similar to attributes, enterprise roles will be required for clouds to make intelligent access control decisions and to enforce policy and otherwise perform fine grained authorization. Currently enterprises maintain user attributes and roles in their on-premise directories such as Active Directory. However, they are required to manually replicate this data into each cloud provider. Current standardization efforts are attempting to solve this within the IETF, particularly the Simple Cloud Identity Management (SCIM) working group. Once this standardization is completed, the support for a SCIM endpoint by all clouds is considered to be a must-have requirement.

EDUCATION

An individual's ability to determine if a computing environment is capable of securing applications and data stores requires an understanding of a large amount of technology. Even in relatively small environment, one must understand many aspects of Information Technology to implement a secure system, such as: operating systems capabilities, operating systems setup procedures, application install bases, application security, application usage patterns, security features offered by the operating system, third party security solutions, network topologies, network security features, and a variety of security policies related to the computing environment. Distributed cloud systems based in large data centers magnifies the complexity of securing assets in the computing environment.

We have learned, through subject matter experts on how agencies conduct day to day operations, that the IT person for an agency is often a deputized officer within the agency. We also learned that many times they are taking on IT responsibilities as part of the career development cycle at the agency. These personnel may very well continue with other aspect of the job common to any officer in parallel with their IT responsibilities. This means that the IT person may not always be a career IT professional and the position will turn over at regular intervals. Where will these administrators turn to gain the knowledge needed to make educated decisions on what solutions can be implementation in the cloud? **There is a need to develop a set of reports and training that will help educate personnel on what the technologies are in this space, how they are used, and where they are deployed, especially when it comes to situations where there are many layers to the technology.**

CLOUD CERTIFICATION

Attaining an accreditation from a trusted third party certification body promotes trust that any vendor's solution does what the vendor claims. The need to gain the trust of the consumer market by a cloud vendor is a predominate issue for the migration of services to the cloud. This is evident because of a reluctance of consumers (PS agencies and utility companies in the case of MC and CI systems) to give up control of their data, mostly because they don't know the security and privacy policies of the provider. There is a need for a body that mission critical and critical infrastructure cloud consumers can turn to for privacy and security assessments.

As a part of their initiative, FedRAMP created a third party accreditation program to access CSPs against FedRAMP requirements. In order to obtain FedRAMP Provisional Authorization and be listed as being a FedRAMP compliant CSP, a CSP must go to an accredited third party assessment organization (3PAO) for testing their security controls. For Mission Critical clouds operated by federal agencies, using a FedRAMP compliant vendor will be a must.

The FedRAMP initiative targets federal agencies. However, could state and local authorities also benefit? Each state could initiate its own program similar to FedRAMP, but it would likely lead to redundancy. **An area of concern identified here is a need for certification programs that are endorsed by state and local authorities.**

Network Access Findings

A consistent theme in the interviews was that Security is an end-to-end challenge – the access is as secure as the weakest link in the end to end ecosystem of actors. Access connection may involve several players of the eco

system. Each has a role to play in securing the data. Customer have to take steps to protect their premise infrastructure, access credentials and take steps to encrypt data, Service Providers have to protect their infrastructure of links and network elements, and cloud operators have to protect the access into them and the service they are providing. As example, DNS is mentioned as the most vulnerable part in the access. Anything done to strengthen the protection will benefit access security. Today, there are no minimum uniform standards for each of the players. Another potentially vulnerable portion of the ecosystem is BGP Hijacking, or the Man-In-The Middle dilemma. Traffic routed over the public Internet to highly susceptible to being hijacked, diverted to an alternative location to be analyzed, and then returned to its final destination – all while the user is completely unaware that this is happening. Securing Internet routing is a growing concern for all Network Access Service Providers when it comes to protecting all forms of consumer data.

One recent article in the media entitled Repeated Attacks Hijack Huge Chunks of Internet Traffic clearly articulates this growing issue.

Currently there does not seem to be a clear demarcation of accountability for the security of data in the cloud between the data owner and cloud operator. In interviews with industry practitioners, it was mentioned that cloud operators take care of VM Down and data owners VM Up. This is an area where clarity may be beneficial. Another remark was about the need for the Data Owners to have visibility to profile and pattern of access to their data. It is not clear how universally this is provided by cloud operators to the data owners. Here again, depending on services accessed (IaaS, PaaS, SaaS) accountability seems to be different.

1. Data across network access to/from the Cloud
    a. Need increased visibility in both performance across the network access as well as transparency as to how data is being handled within the cloud
    b. Increased definition between regulations at the state level vs. the federal level.

2. Security
    a. Sentiment of “we don’t know what we don’t know” from the enterprise when asking, “what’s your biggest concern when outsourcing to the Cloud?”
    b. False sense of security that the Cloud Provider actually has better security protections in place because they are “bigger and must have more knowledge than my team”
    c. CIOs taking the position that they don’t want the gaps in security proactively identified; if they are they’ll be “forced to act”.
    d. Malicious attacks aren’t just working to get into the data from the outside – more attacks are being seen from inside the Virtual Machine (VM) out to other machines. This is causing multiple VMs to have all computing resources consumed and rendering separate customer applications to not function properly

3. Accountability
    a. Identify who is ultimately responsible for the protection of the data as well as the security of the network access.
    b. Accountability should be with the Cloud Consumer to understand not only the protection mechanisms available, but also understand how they should ensure their data is protected (e.g. secure access, encrypted tunnels, virtual firewalls, and encrypted drives). Education of all consumers as well as certification of Cloud Providers are necessary for increasing the protection of and access to data stored within Cloud Networking infrastructure.

Just because the total cost of an outsourced service continues to decrease does not absolve the information owner to ensure the data is secure.

6. CONCLUSIONS AND RECOMMENDATIONS

The impact of cloud computing on the future of information technology cannot be overstated. In the mobile broadband enabled world, cloud computing increasingly provides the foundation of future services for consumers, enterprises, governments, and critical infrastructure. Therefore, ensuring the security and reliability of this pervasively developing paradigm is crucial for the economic viability our country and the safety of our citizens. The FCC is wise in requesting its TAC to assess the landscape of cloud security to determine what activities it may undertake to advance the security and reliability cloud security. The analysis summarized in this paper clearly shows the complexity and diversity of the topic. It also points out that there is an enormous amount of activity in industry, government and academia around the topic of cloud security.

On one hand, cloud security poses an opportunity to raise the overall security level of service by providing users large and small with access to state of the art resources that are managed professionally and with large scale in the industry. In today's rapidly evolving cyber security threat environment, this scale and aggregation of competence is a significant point of leverage such that individual services may not be as subject to the quality and competence of a myriad of organizations faced with economic tradeoffs associated with rigor and currency of their own infrastructure. On the other hand, aggregation of such scale creates a greater dependence on fewer providers for services and each provider increasingly holds more and more responsibility overall. Such dependence increases the 'attractiveness' of large entities as 'targets' for cyber-attack so while the leverage is higher in the hands of a few, the risk factor and threat profile also increase. As a result of this dichotomy, a careful balance must be struck between augmenting and advancing the security and resilience of cloud based services without stifling the advance of this important point of leverage with undo regulation and requirements.

Based upon the analysis described thus far, we conclude that there are four main areas of concern that cut across Consumer and Enterprise, Critical Infrastructure and Network Access.

- Accountability
- Education
- Industry Collaboration
- Certification and Auditing

In the following sections we offer our analysis and recommendations to the FCC in each of these four areas for their consideration in improving and advancing cloud based security across industry and government. Because of the ever increasing dependency upon cloud computing, we also recommend that the FCC commission the 2014 TAC to extend this analysis beyond security to also address considerations associated with the resilience and robustness of cloud infrastructure.

ACCOUNTABILITY

ANALYSIS

Accountability specifies who is responsible for what in the domain of cloud security, how well the expectations on the different attributes will be delivered and what the recourse is if the expectations are not fulfilled. Service Level Agreement (SLA) between actors of the cloud ecosystem is an instantiation of this accountability. As in the saying "good fence makes good neighbors", well-crafted SLA can help make the relations between actors smooth and effective. Currently, SLAs for IaaS is better than PaaS and SaaS although good progress is being made in these areas as well. Larger customers of CSP have a better chance of influencing the SLA provided to them by CSPs. A Cloud Consumer may have SLA with more than one ecosystem actor.

Knowledge or understanding of Accountability is limited when outsourcing to cloud, especially in the SMB area. Often, there is a sense of false security in potential consumers that cloud providers know better, and data and application are more secure and CSP is accountable. Although it may be true in some cases, Consumers have to realize that the ecosystem has several actors – Cloud Consumer, Cloud Carrier, Cloud Service Provider etc. If they have vulnerabilities in their internal operation, moving to cloud may carry the same vulnerability into the cloud environment as well. In the area of auditing and SLA, many documented challenges have come not from a cloud provider's ability to service a customer, but the ability of the customer's systems to interface properly with the cloud**.** Security is as strong as the weakest link in the chain. Each actor has a role to play and has specific responsibilities. Consumer has to perform due diligence before placing his application and data in the cloud and during the time of consumption of cloud services. Although Cloud can offer agility, elastic capacity and cost reduction, potential Cloud Consumer has to fully comprehend the suitability of cloud for his business needs, legal requirements, the impact of the cloud environment on his business, including people, processes and systems and determine the service and deployment model. With this preparation, Consumer can evaluate offers from different CSPs.

An ideal SLA should cover several attributes such as operational (e.g. performance, incident handling, monitoring and reporting, availability, support and escalation, speed of provisioning), security and privacy, standards adhered to, and compliance CSP meets. Consumer has to specially recognize any differences in security in cloud *vis-a-vis* internal IT. "Some of the security risks associated with cloud computing are unique, partly due to an extended data centric chain of custody, and it is in this context that the business continuity, disaster recovery, and traditional security environments of a cloud service provider need to be assessed thoroughly and in reference to industry standards" [1]. Consumer has to recognize that he may bear sole responsibility or share with other players for application and data security depending on the service model and who is the "custodian" of the data.

RECOMMENDATIONS

Short term recommendations

The following recommendations could be thought of as "low hanging fruit" for the FCC to consider. These should be actionable in a more timely manner than the longer term recommendations appearing later in this section.

Short Term Recommendation	FCC Action
1) Develop easy-to-access and easy-to-understand content to make Cloud Consumers aware of – the need for and attributes of various domains of an SLA between ecosystem players and dependency on the service model, since Accountability (expectations and recourse) is captured in SLA[16,17] – the need to evaluate suitability of cloud for their business needs and to conduct due diligence to evaluate security capabilities (e.g. compliance certificates, audit reports, BC / DR) of cloud ecosystem players for all the layers of the "stack" for migrating to the cloud, being in the cloud and exiting from the cloud	Leverage the existing content and collaborate with the industry to propagate

Long term recommendations

The following actions are ones that will take some time to implement and are worthy of future work group focus. Some recommendations could be implemented over the 2014 time frame where others might require longer term plans to implement. There are four long term recommendations that were a result of the 2013 working group.

Long Term Recommendations	FCC Action
1) Study any specific recommendations that may need to be developed for Critical Infrastructure cloud services	2014 study item for TAC ?
2) Extend the scope of Accountability beyond security to other areas such as availability and performance	2014 study item for TAC?

[16] Practical Guide to Cloud Service Level Agreements Version 1.0 Cloud Standards Customer Council, April 10, 2012

[17] Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0, Cloud Security Alliance 2011

3) Study the impact of new SDN / NFV technologies on Cloud security implications and update these recommendations	2014 study item for TAC?

EDUCATION

ANALYSIS

Education is the cornerstone to expand use of the cloud and to protect the security of the networks. As the staff's education on cloud improves, staff and management for an organization can begin to make relatively informed decisions on cloud security and efficiently determine where resources need to be applied to meet the higher risk threats.

For larger organizations with more than five IT staff members, understanding the ever-changing requirements for cloud security is a challenge. Smaller enterprise cloud users are eager to learn however will lack the time commitment and in many cases the core knowledge to assess the needs for security. Currently, these users have to research through volumes of many materials from manufacturers, government or industry association websites to grasp the concepts. The information for these sites is typically not targeted for the small user. Much of the information is designed for a variety of audiences and can be too technical, marketing hype, or in a high-level form.

It can be difficult for the untrained security individual to grasp the major points of security concerns from multiple locations and to apply them to their general needs. Reviewing the available voluminous data is like trying to drink from a fire hose causing an overload of information.

In order to provide highly useful education material, an overall reference guide needs to be developed. The reference guide would include summaries from large, detailed documents for the users with the links to the direct resource. The educational document could also provide case studies for different types of users of the cloud describing the security concerns and generically provide ways to consider removing specific security threats.

A group meeting with enterprise businesses, cloud carriers, government entities, associations and broadband providers could identify gaps in what cloud services have to offer and security concerns associated with each type of usage.

Partnerships with major industry players and NIST content could be created specifically for those in need of cloud security. The information would need to be housed and quarterly maintained by all participants for use by all industries.

The stakeholders could ensure the reference guide becomes common knowledge among the most users in the industry. The cloud and broadband providers could ensure visibility by publicly placing links to reference guides on websites for consumers' use.

Government agencies could ensure the information is made available to users of the many government programs. These agencies could provide the links or add information specific to programs under their purview for added value.

The development of a reference guide will require ongoing support and commitment by all involved to ensure quarterly updates are made to cover new issues of concern.

One agency or group needs to take the responsibility to institute the educational guide and ensure timely updates will continue for the long-term use in the cloud marketplace

RECOMENDATIONS

Short-term recommendations

The following recommendations could be thought of as "low hanging fruit" for the FCC to consider. These should be actionable in a more timely manner than the longer-term recommendations appearing later in this section.

Short Term Recommendation	FCC Action
1) Collaborate with industry and academia to identify best Education & Awareness materials for use	FCC to coordinate the process and qualify work to ensure desired results
2) Materials should be evangelized	FCC to place information on website
3) Update older material to make relevant	FCC to use labor resources to determine what material is obsolete and determine how to improve its relevance
4) Develop a website reference for small enterprise users	FCC to work with other stake holders to incorporate materials from other sources into a useful reference guide source for small businesses

Long-term recommendations

The following actions are ones that will take some time to implement and are worthy of future work group focus. Some recommendations could be implemented over the 2014 time frame where others might require longer term plans to implement. There are four long-term recommendations that were a result of the 2013 working group.

Long Term Recommendations	FCC Action
1) Identify gaps in Education & Awareness material	FCC to lead work on the continued construction of useful documents for cloud users and corresponding security concerns
2) Hold workshops to increase Education &	FCC to create a strategy for the development and

Awareness	sustainability of published materials
3) Public Awareness	FCC to continue labor investment in updates, develop liaisons with other governmental agencies to have the updated referenced material posted on websites and disseminated to users. Include entities such as SBA, USDA, NTIA Cloud providers, Industry Associations, Smart Communities and Broadband Providers
4) Provide information to Cloud and Broadband Providers for placement on websites for consumer's usage	FCC to disseminate information to the communication providers to lead the industry in the placement of material on websites for public consumption.

INDUSTRY COLLABORATION

ANALYSIS

With 95% of the nation's critical infrastructure owned and operated by the private sector, industry collaboration on network access, resiliency, and cyber security is essential. This collaboration includes both industry cooperation between owners and operators of national Information Technology assets, and effective communication and cooperation between the private sector and the public sector on the shared priorities of information security, integrity, and availability. In this view, industry collaboration functions as a central tenet in the multi-stakeholder approach to Internet governance broadly, and network access and security specifically.

Certainly, both the legislative and the Executive Branches of government have established many federal agency roles and recommendations in this space that reflect the government's interest in (and commitment to) secure IT systems, including Cloud Computing. For example, the National Institute of Standards and Technology (NIST, within the Dept. of Commerce) has the lead role in developing cloud computing definitions and standards, promoting key areas of interest, and creating a incentives for technology standards adoption; the General Services Administration (GSA) leads the Government's efforts to educate federal departments and agencies about operating standards and adoption best practices for Cloud Computing; and the Office of Management and Budget (OMB) is tasked with setting the national agenda for secure network and data integrity priorities. One of GSA's projects in this role, as directed by the Federal CIO Council, was to establish and lead the Federal Risk and Authorization Management Program (FedRAMP).[18]

Recent examples of governmental critical infrastructure and information security initiatives demonstrate that these actions are both influenced by industry and significantly influence industry. In the past seven years, for example, network access and security initiatives by government that have been supported by (and have heavily impacted) ongoing private sector collaboration initiatives include:

- 2007, Government establishes Trusted Internet Connection (TIC) program
- 2009, President establishes first-ever Federal Chief Information Officer (CIO)
- 2010, Federal CIO establishes Federal Data Center Consolidation Initiative (FDCCI)
- 2011, OMB launches "Cloud First" initiative prioritizing info security, access, and $ savings
- 2012, Government expands "Bring Your Own Device" initiative for data access, security
- 2013, President releases Executive Order 13636, "Improving Critical Infrastructure Cyber Security, including NIST-led industry collaboration for access & security standards[19]

At each of these points of interface with the government, industry convenes and collaborates with the government to develop best practices and performance standards to advance network access and information security. And behind the scenes of this two-way information flow with government, industry works together across corporate

[18] For more on these and other examples, see "NSTAC Report to the President on Cloud Computing" (p. 3) published May 2012 by the National Security Telecommunications Advisory Council, available at DHS.gov/NSTAC

[19] For more on these and other examples, see "NSTAC Report to the President on Secure Government Communications" (p. 3), published August 2013 by NSTAC, available at DHS.gov/NSTAC

boundaries to promote clarity and consistency in the insights it shares with government, and to promote transparency and effectiveness in implementing the guidance that government shared with industry.

Underlying this model, industry collaboration takes three primary forms:

- Industry-to-industry collaboration, industry-organized, & industry-led
- Industry-sponsored collaboration that funnels guidance to government
- Government-sponsored entities that foster/facilitate industry input

There are many best practices and examples of excellence in each of these models of industry collaboration,that vary according to the customer profiles, the product offerings, and the company priorities. Just two examples from each model, however, can help illustrate the diversity, including:

- Industry-to-Industry Collaboration:
    - Information Technology Industry Council (ITI) links policymakers, companies, and non-governmental organizations to advance standards, cooperation, and interoperability.
    - TechAmerica fosters comprehensive global, national, and regional advocacy and high-level policy and technology collaboration establishing standards and transparency in the ICT industry.
- Industry-sponsored collaboration that funnels guidance to government:
    - Sector Coordinating Councils (such as the IT-SCC) that develop standards and foster peer review and transparency standards for Service Level Agreement elements such as access & up-time
    - Information Sharing & Analysis Centers (ISACs) that facilitate the exchange of both classified and unclassified cyber security information including known threats and detection techniques
- Government-sponsored entities that foster and facilitate industry input
    - Presidential advisory panels such as National Security Telecommunications Advisory Council (NSTAC), with recent reports on Cloud Security, FirstNet, and Secure Gov't Communications
    - National Institute for Standards & Technology (NIST), currently leading industry collaboration efforts for standards and incentives ensuring network access and security

RECOMENDATIONS

Short term recommendations

The following recommendations could be thought of as "low hanging fruit" for the FCC to consider. These should be actionable in a more timely manner than the longer term recommendations appearing later in this section.

Short Term Recommendation	FCC Action
1) Existing best practices in the development and adoption of network access & security standards can be supported and enhanced by the FCC	The TAC recommends incorporating network access and security education and awareness "toolkit" information into 2014 FCC meetings with industry partners and other stakeholders throughout 2014.

2) The FCC has unique convening capability to facilitate industry collaboration and cooperation. Although Legislative and Executive branch policy puts regulatory jurisdiction elsewhere, the FCC can build and nurture industry collaboration among key stakeholders by prioritizing critical infrastructure network access and security in the coming year.	The TAC recommends the FCC consider holding public-private partnership workshops in 2014 that gather and disseminate network & access standards, and facilitate interaction among a wider diversity of industry partners to continue to improve both security standards and the standards development process.

Long term recommendations

The following actions are ones that will take some time to implement and are worthy of future work group focus. Some recommendations could be implemented over the 2014 time frame where others might require longer term plans to implement. There are four long term recommendations that were a result of the 2013 working group.

Long Term Recommendations	FCC Action
1) As Cloud Computing grows ever-more ubiquitous, the range of consumers and enterprises that utilize the platforms of IaaS, Paas, and Saas will also continue to broaden. This will likely lead to an ongoing growth in the number of government entities that have an interest in ensuring the integrity, security, and availability the systems and of information to Cloud customers. Because the FCC has a unique and diverse set of stakeholders, cooperation with other government entities will be required to ensure clarity and consistency in government's work in this area.	The TAC recommends the FCC partner with other federal government entities & agencies overseeing network access and cyber security issues (such as DHS, NIST, WH/OMB) to ensure the transparent, collaborative development and effective industry adoption of network access & security standards. For example the FCC might collaborate with NIST to further promote and advance NIST's Cyber Security Framework.
2) As the ecosystem of Cloud Computing customers and providers continues to expand, the need for efficient and effective information sharing to ensure network access and security will	The TAC recommends that the FCC plan and establish an FCC-convened "clean room" for information sharing among and between its diverse landscape of stakeholders, allowing the

grow. Horizontally both between enterprise customer sets and among industry colleagues and competitors; vertically, and bi-directionally, between industry and government; and on an ongoing basis moving forward in time, there is a need for a safe space for sharing information across the diverse range of FCC stakeholders.	secure, efficient, and effective sharing and distribution of accurate and actionable network access and information security details including threat signatures, security standards, cyber security frameworks and other best practices.[20]

[20] For more discussion on this recommendation, see FCC Technical Advisory Council Summary of Meeting minutes, Sept. 24, 2012, p. 2 (available at http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92412/meeting-minutes-9-24-12.pdf).

CERTIFICATION & AUDITING

ANALYSIS

This section contains an analysis of best practices for cloud certifications as they are applied to Commercial, Federal Government and Utility companies. The discussion includes areas where there is good coverage and where additional efforts could help boost customer confidence and improve adoption of cloud technologies. Any general areas of concern noted herein, that result in slow cloud adoption, were gathered from independent analysis as well as discussions with industry experts, state CIOs and utility companies. This analysis is limited to security aspects of certification.

Today there exist frameworks/architectures that can be used to help improve general understanding of cloud security issues. For example, NIST SP 500-292 describes a high level architecture for clouds and NIST SP 500-299 describes a security architecture that is an overlay for SP 500-292. SP 500-299 was sent out for comment in June of 2013. Cloud Service Providers can also complete a Service Organization Control (SOC2) certification audit that evaluates internal controls based on five key control principles: security, availability, processing integrity, confidentiality and privacy. The SOC 2 audit program is maintained by the AICPA. These reports can be used by cloud security enterprise consumers (enterprises, government, etc.) to assess and address risk associated with outsourcing a service to an entity such as a cloud provider. SOC2 is not a cloud specific evaluation but serves the space well.

In addition to frameworks for clouds and security controls for service organizations, the analysis for certification and auditing uncovered areas where existing certifications are serving aspects of 4 areas of study: Enterprise/Consumer, Federal Government, Mission Critical and Critical Infrastructure.

Third party commercial cloud audit solutions are relatively new and beginning to gain popularity. The AICPA introduced a new audit framework designed to help evaluate cloud service providers in 2012 using five audit trust principles. The CSA's Security, Trust & Assurance Registry (STAR) is a method of improving transparency with respect to cloud environments. The STAR program uses the Open Certification Framework (OCF) to improve trust in the cloud for enterprise markets by offering transparency and assurance methods. There are two current program levels and one future program level planned as part of CSA's STAR certification program:

- Level 1 (Current)– Cloud service provider performs a self-assessment using the CSA's Cloud Control Matrix (CCM).
- Level 2 (Current) - STAR Certification / Attestation is a third party assessment of controls described in the cloud service provider's CCM using ISO27001 or AICPA SOC2 audit methodology.
- Level 3 (Future) - STAR Continuous is a publication report based on continuous security monitoring of the cloud provider using the Cloud Trust Protocol (CTP).

CSA launched the level 2 program in September 2013. Many major CSPs have begun certification exercised to attain Level 2 certification as a part of their compliance efforts. As part of its Level 2 is a third party evaluation program, CSA also maintains a list of third party assessors. It should be mentioned that there is currently one company (British Standards Institute) listed as official third party assessors for CSA STAR program. However, it is expected that that list will grow over time.

Audit certification frameworks like SOC2 and CSA STAR offer controls assessments for cloud service providers that were not available a few years ago. Although these certification frameworks are promising, time will tell whether or not these programs will deliver the types of assurance enterprises need to evaluate CSPs.

AICPA SOC2 reports have become the popular industry standard for IaaS and SaaS providers servicing more discerning enterprise customers. Many cloud service providers already deliver SOC2 reports that audit security and availability. Often SOC2 reports deliver a limited scope of physical and logical security delivered as part of the CSP's cloud service. Without skilled expertise, enterprises often are unable to evaluate whether or not SOC 2 controls will help reduce risk in the cloud.

As part of CSA's cloud certification program, over 40 CSPs have submitted CSA's Level 1 STAR self-assessments. Time will tell if Level 2 certifications will become common practice among cloud service providers. As of the date of this publication, no providers have achieved Level 2 status (although the program is new).

Today, many consumer/enterprise grade cloud solutions rely on hybrid cloud delivery models – where for example one provider delivers an enterprise application that is hosted on another provider's cloud infrastructure. These models blur the lines of responsibility because they require a complex, interdependent controls structure to properly protect the enterprise customer. Unsuspecting consumer/enterprise consumers may be unaware of the delivery model and the potentially complicated security and privacy implications of a hybrid delivery model. In a hybrid model, controlling and restricting access to data may require close collaboration between two or more entities. Should one entity fail to adequately implement or maintain controls, it may introduce security or privacy risk to its consumer or enterprise customers.

CSPs that wish to sell services to the federal government must acquire an Authority To Operate (ATO) under the Federal Risk and Authorization Management Program (FedRAMP) from either a sponsoring agency or the Joint Authorization Board (JAB). FedRAMP's security controls are based on NIST SP 800-53. The FedRAMP program continuously updates its security baseline. In July, FedRAMP recently distributed a security baseline update for public comment as a part of their continuous improvement program. FedRAMP's recent updates are based on version 4 of NIST SP800-53.

Two general observations come to mind with respect to the state of the industry today. First, cloud frameworks are relatively new. As these frameworks evolve and become widely adopted, they will be more capable of providing the continuous monitoring and transparency needed to improve trust in cloud solutions. The Second general observation is that evaluating CSPs is a generally rigorous, resource intensive and complex process. Successful evaluation programs favor large enterprise and large government agencies with the budget to support large IT staffs. Smaller enterprises/entities will have more difficulty evaluating CSPs since they typically are unable to support major efforts adequately assess risk when selecting a cloud provider.

In addition to the general observations made above, the analysis conducted revealed a number of areas of that were not covered by existing programs. For example in the government space, state and local agencies lack a certification body, such as FedRAMP for the federal space, to help assure a consistent set of security controls are in place. Discussions with state CIOs and state and local IT departments give us a good indication that efforts to cover certifications for these entities should be sponsored at the federal level.

The team also looked at potential adoption of cloud technologies by agencies supporting public safety and first responders (aka Mission Critical systems). These entities were predominately focused on evaluating a CSP's ability

to deliver resilient cloud applications and infrastructure to support high availability, privacy, transparency and access control requirements. The certification model used by CSPs under FedRAMP may be an excellent model for delivering many mission critical systems. FedRAMP defines security controls and requirements for system confidentiality, integrity and availability based on the sensitivity of data stored and maintained by the application/cloud service. Currently, FedRAMP only covers certifications for CSPs that can support systems that maintain "low and moderate" impact data (as defined by FIPS 199/200). The challenge arises when considering the protection and security of critical law enforcement data, locally created data, other agency sourced data such as the Federal Bureau of Investigations' databases. Not only must this data be available 24 hours a day, 7 days a week and 365 days a year, but the data owner must also show proper chain of custody for the data. Additionally Criminal Justice Information (CJI) is governed by policy, specifically the Criminal Justice Information Services (CJIS) Security Policy. Handlers of this data must not only attest to controls required by current policy but also agree to implement any new controls as they evolve over time. If one were to evaluate CJI data using the methods contained within FIPS 199, they would conclude that CJI data is "high" impact data and therefore not covered by programs like FedRAMP. Our informal interviews and discussions lead us to believe that public Safety entities desire a certification program in this area for complete coverage.

Critical infrastructure providers (utilities, telecommunications companies) have additional requirements or regulations that require them to ensure resiliency and security of key control systems in their environment. Current security requirements (e.g. NERC CIP) are punitive instead of supportive and the CI entities have little incentive to move applications to the cloud. From the data we gathered, it appeared that CI entities were considering three general categories of services to move to the cloud: non-mission critical (e.g. human resources), billing data, and to a lesser extent, SCADA. There were varying levels of migration to the cloud for non-mission critical but all of the contacted entities either expressed interest or were in the process of moving those services to the cloud. The CI companies were skeptical that they could move billing services to the cloud, as they were heavily customized and complex in-house applications.

None of the CI companies we talked to had any plans on moving SCADA to the cloud as they have a mix of legacy devices and applications with widely varying levels of security. However, there are solution providers connecting physical security systems, PLCs, etc. to cloud-based back-ends for management. For example, one vendor offering automating to SCADA networks is Digi's Cloud solutions at http://www.digi.com.

RECOMENDATIONS

One must consider a variety of factors to understand what controls would be needed to secure any cloud implementation for a give vertical. Risk of data exposure, regulations and price, just to name a few, will need to be considered to find a solution that fits the need. Each vertical discussed in this paper (consumer, enterprise, mission critical and critical infrastructure) have implementations that require different levels of controls. Within each vertical multiple levels of assurance will be needed to enable pricing that would benefit the consumer. The reality of the situation is that driving a strict and heavy certification process across all market will push up price points and negatively impact the space.

After scanning the industry over the past year it was realized that a "one size fits all" solution does not exist for cloud services. Heavily controlled environments will not meet price points for consumer and small enterprise efforts, nor will cheap services meet strict controls required for public safety environments. This does not mean that we are starting from scratch, so to say, when addressing certifications for cloud providers. There are existing

certifications and requirements that should be leveraged as a part of any action taken by the FCC in this area of focus. Included in this list of existing foundations to build on are:

- ISO 27001/2
- NIST 800-53
- AICPA/SOC2
- FedRAMP (Certification Body)
- STAR Registry

In fact the enterprise market is well covered by the evolving CSA Open Certification Framework. The three levels of Open Certification Framework that are a part of the STARs program are well suited to enterprise cloud service customers.

Short term recommendations

The following recommendations could be thought of as "low hanging fruit" for the FCC to consider. These should be actionable in a more timely manner than the longer term recommendations appearing later in this section.

Short Term Recommendation	FCC Action
1) As a recommended best-practice, all enterprises and organizations should conduct an application audit concurrent with moving to the cloud.	FCC sponsored workshop to explore public/private partnership to promote application security in the cloud, enhanced application security in the cloud translates to fewer targets for hackers, cleaner network traffic, and fewer threats to critical infrastructure.

2) Leverage existing standards for certification, and existing certification bodies, to help educate potential cloud service consumers.	Provide guidance and education on the following:
	• Security controls and guidance documents
	  • NIST SP 500-292 and NIST SP 500-299
	  • NIST SP 800-53 and FIPS 199/200
	• Certification standards
	  • AICPA SOC2
	  • ISO 27001, 27002
	• Certification bodies
	  • FedRAMP
	• Certification frameworks
	  • CSA Open Certification Framework

Short term action 1: Our analysis has indicated that despite the volumes of educational material that has been published in the last five years about cloud security, there still major gaps between awareness and practice still

exist today. Many cloud adopters lack the awareness and skills to evaluate and address security vulnerabilities in their applications before they are migrated to the cloud. Enhanced application security in the cloud translates to fewer targets for hackers, more stable communications infrastructure, and fewer threats to critical infrastructure. The TAC recommends that the FCC sponsor workshops to explore public/private partnership that can promote application security in the cloud.

Short term action 2: The FCC could help improve public awareness of security controls, certification standards and certification bodies through education of potential cloud service consumers. The specific actions could be to provide guidance and education on efforts by NIST who has published SP 500-292, which is a standard cloud framework document, and SP 500-299, which is a security overlay to the cloud framework. NIST has also published a set of security controls in SP 800-53 and a data method for data characterization in FIPS 199 and 200. The former set is used by FedRAMP as a part of their authority to operate. Finally as a part of this action, the FCC should educate the public on CSA's Open Certification Framework. This framework is designed to help improve trust and transparency of the cloud providers.

Long term recommendations

The following actions are ones that will take some time to implement and are worthy of future work group focus. Some recommendations could be implemented over the 2014 time frame where others might require longer term plans to implement. There are four long term recommendations that were a result of the 2013 working group.

Long Term Recommendations	FCC Action
1) Closely evaluate existing certification standards for security gaps.	Collaborate with the CSA to drill down on security standards to address any gaps that may exist as a 2014 standards
2) Leverage the FedRAMP certification process for state and local agencies	Reach out to FedRAMP to expand coverage to state and local agency certifications.
3) Create certifications for CJIS data service providers	Reach out to FedRAMP to expand coverage for CJIS and High Impact Data coverage Alternatively, address high impact needs via the sponsoring of Community Clouds for PS/State/Local
4) Create a Certification Body that cover NERC-CIP requirements for CI	Reach out to NERC to extend compliance standards to cloud providers for CI data

Long term action 1: The FCC could help evaluate existing certification standards for security gaps that might prevent adoption of cloud services. Specifically the FCC could collaborate with the CSA to drill down on security

standards to identify and address any gaps in the existing standards. The results of this effort would be reflected in level 1 and level 2 certifications and attestations. The level of effort to complete this work would fit nicely in the time allotted to annual work group activities. As it exists today, security standards documents are continually evolving and this is an area where the FCC could lend assistance.

Long term action 2: As it was discussed in the analysis section, state and local governments lack a certification body to turn to when trying to evaluate cloud services. The desire to reduce cost and move to the cloud exists but the lack of confidence in solutions and the ability to customize SLAs is not. The FCC could help by working with an existing certification body to get a program put in place for state and local governments. Specifically, the FCC should reach out to FedRAMP and work with them to extend coverage of the program to state and local agencies.

Long term action 3: In a similar situation to the recommendation above, we are not aware of a certification program specifically designed to handle highly sensitive CJI data. The FCC could facilitate change in this space by working to create or better yet augment a certification body to cover CJI data. The FCC should reach out to FedRAMP to facilitate changes within that program to include certification for CJI data, possibly as a new authority to operate within FedRAMP. As an alternative to working FedRAMP, the FCC could sponsor community clouds that are designed to meet CJIS requirements.

Long term action 4: Utility companies operating systems that are regulated by NERC-CIP requirement for CI. They are very hesitant to move data services to the cloud because disruption or compromised can result in fines to the utility company. We are not aware of certification bodies that cover cloud implementations for critical infrastructure and the FCC could help create certifications appropriate to this space. The FCC should reach out to NERC to work with them to extend compliance standards to cloud providers for CI data.

7. APPENDICES

Appendix 1: Current Industry/Government Initiatives to Address Gaps

The areas of concern discussed in Sections 4, 5, and 6 above, when viewed by both industry and government, provide insights for opportunities and directions for initiatives to address these topics. Four distinct processes are underway, from a range of entities, which attempt to do address these topics, including policies and pronouncements from the Executive Branch; programs and standards protocols from Executive Branch agencies; guidance and recommendations from the private sector; and evaluation and analysis from the nonprofit sector.

Examples of each of each of these efforts include:

Executive Branch/Presidential:

Executive Order 13636 (Improving Critical Infrastructure Cyber-security) directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

[See: http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical]

Presidential Policy Directive-21 (Critical Infrastructure Security and Resilience) replaces Homeland Security Presidential Directive 7 and directs the Executive Branch to:

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan

[See: http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical:]

These directives are important because they chartered NIST to develop a voluntary framework for reducing cyber risks to critical infrastructure. Critical infrastructure is defined as systems critical to the country's security, including economic and public health safety. This includes the growing reliance on cloud services. The NIST framework is designed to help infrastructure owners and operators manage cyber-security related risk while protecting business confidentiality, individual privacy and civil liberties. As a part of this voluntary standard, NIST published the following documents related to clouds and cloud security.

- NIST SP 500-291 "NIST Cloud Computing Standards Roadmap"
- NIST SP 500-292 "NIST Cloud Computing Reference Architecture"
- NIST SP 500-299 "NIST Cloud Computing Security Reference Architecture"

[Citation: http://www.nist.gov/itl/csd/cybersecurity-041713.cfm] Recent activity includes a workshop held by NIST at the University of North Carolina on the cyber-security frame work. The workshop was held on November 14, 2013 [Citation: http://www.nist.gov/itl/csd/5th-cybersecurity-framework-workshop-november-14-15-2013.cfm]

Collaboration between GSA, NIST, DHS, DOD, NSA, OMB, Federal CIO Council

In an effort to facilitate the " cloud first" directive issued by Federal CIO Vivek Kundra, GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council, and various members of the private sector formed the Federal Risk and Authorization Management Program (FedRAMP). This program is designed as a standard approach to acquiring cloud services for federal agencies. This body maintains a list of vendors that have been given the authority to operate either provisionally by the Joint Authorization Board or more formally by the agencies. The difference being that it is ultimately the agency that is responsible for their compliance under FISMA (Federal Information Security Management Act) and therefore the agency is the one who decides if a CSP gets the Authority to Operate (ATO). FedRAMP is essentially a tool to speed the process of getting the ATO from an agency.

FedRAMP uses NIST control documents to access the viability of the CSP. Specifically, FedRAMP uses NIST 800-53 "Recommended Security Controls for Federal Information Systems and Organizations" as the set of controls that must be met by a cloud provider before considering them for an ATO. FedRAMP uses FIPS 199/200 as a data classification standard. These documents categorize data into low, moderate and high impact levels. FedRAMP only covers low and moderate impact levels of data.

IACP

The International Association of Chiefs of Police (IACP) /SafeGov/Ponemon Institute conducted a survey of IACP member agencies examining how local and state law enforcement officials would use cloud services. They subsequently published a summary of those results. The survey's goal was to gauge the perception of the community on the potential of cloud computing in the law enforcement environments and any future cloud usage plans.

The IACP released a set of guidelines for using the cloud for CJIS data in January 2013 at the Leveraging the Cloud for Law Enforcement Symposium. The document was developed in collaboration with key law enforcement subject matter experts. They are currently in the process of updating the document "Guiding Principles on Cloud Computing in Law Enforcement" based on comments after its release.

CJIS Addendum

All Criminal Justice Information (CJI) data is controlled under the "Criminal Justice Information Services (CJIS) Security Policy". This policy describes what constitutes CJI data and how it must be protected. A new version of the CJIS document has recently been published (Criminal Justice Information Services Security Policy Version 5.2). Section G3 is a new addendum that discuses CJIS in the cloud.

NERC CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) provides a suite of standards that ensure the overall security of computing systems that directly manage power grids and associated systems. Critical Infrastructure security controls include NERC-CIP and NISTIR (National Institute of Standards and Technology Interagency Report) 7628. Though these are not focused on the cloud, they will likely need to be met by any CSP operating in this space.

CSA

The Cloud Security Alliance (CSA) hosts the Security, Trust and Assurance Registry (STAR). This program is designed to improve customer confidence and transparency with respect to cloud services using the Open Certification Framework (OCF). There are three levels of attestation to this program (Self, Third Party and Continuous Monitoring). The self-assessments are based on Consensus Assessment Initiative (CAI) Questionnaire and/or Cloud Control Matrix (CCM). The third party assessment is based the Cloud Control Matrix (CCM) and ISO27001/2 or AICPA SOC2. The continuous monitoring piece of the program is based on Cloud Trust Protocol (CTP).

The Cloud Control Matrix (CCM) established by the Cloud Security Alliance (CSA) is an assessment tool to help cloud providers understand CSA's security controls and aid cloud consumers with overall assessment of risk of using any given provider. In short, CCM provides a controls framework designed to help cloud providers and consumers with an understanding of security controls and principles used by the CSA.

ISO27001/27002

The International Organization for Standards (ISO) provides a set of recommendations for information management systems. The recommendations include information security management, risks and controls for what are described as an Information Security Management System (ISMS). Two documents that are used in the cloud environment from the series of document are 27001 and 27002. ISO 27001 is a management standard that describes how an information management system should be run. ISO 27002 describes a set of best practice controls to be used on an information management system.

AICPA SOC2

The American Institute of Certified Public Accountants (AICPA) has developed a set of reports that are designed to give an account of the current set of controls for a service organization. The Service Organization Control (SOC) reports provide information on the internal controls implemented by a service organization to assess the risk of outsourcing any given service. SOC1 is focused on internal controls over financial reporting. SOC2 deals with security, availability, processing integrity, confidentiality & privacy, and thus is more relevant to CSPs. CSPs will typically publish these reports as an attestation of their security controls.

Appendix 2: Government/Industry/Standards Organizations Active with Cloud Security

Government Operational and Capability Responsibilities

• Federal Risk Authorization Management Program – FEDRAMP	http://www.fedramp.net
• National Institute of Science and Technology Cloud Security Working Group - NIST	http://www.nist.gov
• General Services Administration – Cloud Computing Program Management Office	http://www.gsa.gov
• Department of Homeland Security Office of Cyber-Security and Communications	http://www.dhs.gov
• Health and Human Services Office of the CIO	http://www.hhs.gov/ocio/ea
• Defense Information Systems Agency - DISA	http://www.disa.mil
• Office of the Secretary of Defense Chief Information Officer – OSDCIO	http://www.dodcio.defense.gov
• Office of the Director of National Intelligence Chief Information Officer – ODNICIO	http://www.dni.gov
• National Nuclear Security Agency Office of the Chief Technology Officer – NNSA CTO	http://www.nnsa.energy.gov
• Government Chief Information Officer Council	http://www.cio.gov
• European Network and Information Security Agency (ENISA)	http://www.enisa.europa.eu/
• Secure Cloud Computing for Critical Infrastructure IT Consortium	http://www.seccrit.eu/

Government Research Agencies

• The Networking and Information Technology Research and Development Program	http://www.nitrd.gov
• National Science Foundation – Computer & Information Science & Engineering Directorate	http://www.nsf.gov
• Defense Advanced Research Projects Agency – DARPA	http://www.darpa.mil
• Intelligence Advanced Research Projects Agency – IARPA	http://www.iarpa.gov
• Department of Energy Office of the CIO and Office of Science	http://www.doe.gov
• Department of Homeland Security – Science & Technology Directorate	http://www.dhs.gov/st-directorate

Industry Standards Organizations

• Cloud Standards Customer Council – CSCC	http://www.cloud-standards.org
• Openstack	http://www.openstack.org
• W3C	http://www.w3.org/community/cloud
• Organization for the Advancement of Structured Information Standards – Oasis	http://www.oasis-open.org
• Open Services for Lifecycle Collaboration	http://www.open-services.net
• Distributed Management Task Force – DMTF	http://www.dmtf.org
• European Telecommunications Standards Institute – ETSI	http://www.etsi.org
• Global Inter-Cloud Technology Forum – GICTF	http://www.gictf.jp
• Open Grid Forum – OGF	http://www.gridforum.org
• Object Management Group – OMG	http://www.omg.org
• Open Cloud Consortium – OCC	http://www.opencloudconsortium.org
• Storage Networking Industry Association – SNIA	http://www.snia.org
• Tele Management Forum – TM	http://www.tmforum.org
• Telecommunication Industry Association – TIA	http://www.tiaonline.org
• Association for Telecommunications Industry Solutions – ATIS	http://www.atis.org

• The Open Group	http://www.opengroup.org
• Association for Retail Technology Standards – ARTS	http://www.nrf-arts.org
• Cloud Security Alliance – CSA	https://www.cloudsecurityalliance.org
• PCI Security Standards Council – PCISSC	https://www.pcisecuritystandards.org
• Internet Engineering Task Force – IETF	http://www.ietf.org
• Software and Information Industry Association – SIIA	http://www.siia.net
• IEEE Cloud Computing	http://cloudcomputing.ieee.org
• American Institute of CPAs – AICPA	http://www.aicpa.org
• National Defense Industry Association – NDIA	http://www.ndia.org

International Organizations

• European Network and Information Security Agency – ENISA	http://www.enisa.europa.eu
• Intelligent Transportation Systems for Europe – ERTICO	http://www.ertico.com
• European Communications Organization – EURESCOM	http://www.eurescom.eu
• Cloud Computing Association In Taiwan	http://www.twcloud.org.tw/
• Infocomm Development Authority of Singapore – IDA	http://www.ida.gov.sg
• Singapore Economic Development Board – EDB	http://www.edb.gov.sg
• Korean Electronics and Telecommunications Research Institute	http://www.etri.re.kr
• Ministry of Public Security PRC – MPS	http://www.mps.gov.cn
• Office of the Government Chief Information Officer, HK	http://www.ogcio.gov.hk
• European Cloud Partnership	https://ec.europa.eu/digital-agenda
• International Telephone and Telegraph Union Cloud Computing ITU-T	http://www.itu.int/en/ITU-T/jca/Cloud

Appendix: 3 Mission Critical and Critical Infrastructure Security and Privacy Issues from NIST 800-144

The following set of privacy and security related issues are taken from NIST 800-144, "Guidelines on Security and Privacy in Public Cloud Computing and tailored for CI and Mission Critical areas".

Governance - Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. In Mission Critical cloud instantiations, oversight on complex issues such as data sharing to resource allocation in a community cloud will need to be addressed.

Compliance - Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. In CI and Mission Critical, the primary compliance documents are CJIS and FedRAMP. One key compliance area is data location. Cloud data centers are geographically located worldwide. Government data cannot be stored outside the countries boundaries where it is not subject to U.S. law. Situations may exist where subpoenas would force cloud providers to hand over U.S Government data it is stored off shore as the storage facility may be subject to that locality's law. A third party's data center location would impact the ability to offer solutions for Mission Critical and Critical Infrastructure use cases.

Trust - Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. Mechanisms will need to be in place to demonstrate that the cloud provider mitigates insider access to mission critical data, such that the data does not go offshore, and is not leaked to other customers utilizing this cloud instance. Transparency in the way the cloud provider operates, including the provisioning of composite services, is a vital ingredient for effective oversight over system security and privacy by an organization.

Architecture - The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. Therefore, it is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. In the mission critical arena, understanding the interconnections of cloud services will be necessary to provide confidence in the resiliency of the services provided by the cloud. Limitations on network bandwidth during a crisis can prevent cloud services from performing adequately and understanding hardware and network resource demands is key to architecting the system correctly.

Identity and Access Management - The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult. In an emergency situation there may be federal, state, and local entities needing access to cloud services which will require some type of federated identity and access management mechanisms.

Software Isolation - High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. To reach the high scales of consumption desired, cloud providers have to ensure dynamic, flexible delivery of service and isolation of consumer resources. Many threat vectors exist in a shared environment such as the cloud.

Data Protection - Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds. For instance, a threat comes from the fact that an attacker could rent a VM in the cloud and instantly be shoulder to shoulder with the data that they wish to steal. Articles have even been published on techniques an attacker can use to narrow down the search for a target system. Other threats could also come from data artifacts leftover when hard disks are reused in virtual storage services. If data is not securely wiped from the sections of a hard disk, when it is returned to the pool of available resources, data recovery techniques could be used to expose the data.

Another concern over moving critical systems (mission critical and critical infrastructure) to clouds is the exposure to previously private systems to the internet. This concern is exacerbated by instances of cyber-security attacks such as the one experienced by Iran's nuclear program. The Stuxnet worm attacked computers using Windows OS or Siemens industrial software in order to steal data on the system. This was the first suspected instance of an attack by a nation state. In addition, data breaches could lead to loss or modification of critical data. Other threats exist that deal with changing data collected by monitoring units for critical infrastructure. This data modification could lead to situations where hackers can supply control units with modified data that could lead to system damage. Finally concerns over accidental or deliberate modification or deletion of critical data exist with respect to data residing in the cloud. As we consider use cases for mission critical and critical infrastructure the need to make data available and secure is a challenging task for the cloud.

Availability – Availability is the extent to which an organization's full set of computational resources is accessible and usable. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Public Safety applications that use the cloud will need to meet strict availability requirements for 99.999% availability which many cloud vendors support in their service level agreements. Other risks to availability include unplanned downtime and denial of service attacks. For example, in April 2009, the Federal Bureau of Investigation raided computing centers in Texas and seized hundreds of servers, when investigating fraud allegations against a handful of companies that operated out of the centers. The seizure disrupted service to hundreds of other businesses unrelated to the investigation, but who had the misfortune of having their computer operations collocated at the targeted centers.

Incident Response - Incident response involves an organized method for dealing with the consequences of an attack against the security of a computer system. Response to an incident should be handled in a way that limits damage and minimizes recovery time and costs. Collaboration between the cloud consumer and provider in recognizing and responding to an incident is vital to security and privacy in cloud computing. Federal agencies have an obligation to report certain categories of incidents to the U.S. Computer Emergency Readiness Team (US-CERT) within one or two hours of discovery or detection. Security breaches within the CI and mission critical areas could

potentially have a significant impact to the United States security. An example is the above mentioned Stuxnet worm. That attack had the potential of causing grave damage to the area and people within that area.