Expanded Findings Around Mission Critical and Critical Infrastructure Cloud Usage

A More In-Depth Look at the Relevant Use Cases and Areas of Concern

FCC TAC

Communications Infrastructure Security Workgroup

This paper is a supplementary document to the FCC findings paper presented as a part of the deliveries for the 2013 Communications Infrastructure Security TAC working group. It contains expanded descriptions of use cases and areas of concern.

12/09/2013

Contents

1. INTRODUCTION

The FCC-TAC's working group for Communications Infrastructure Security recognized four key vertical markets to consider during their mission to identify the top ten security concerns of cloud computing, as a part of the 2013 effort for the group. The verticals identified and used by the group during the research were Consumer, Enterprise, Mission Critical (MC) and Critical Infrastructure (CI). It was initially assumed that those verticals would have different requirements. As the researched progressed throughout the year, the perceived deltas in the requirements were affirmed.

A couple of factors related to MC and CI gave rise to the need for a deeper dive into the use cases for those two verticals. The two factors are relatively slow adoption of cloud usage and tighter security requirements, the former being causally related to the later. The team felt that expanded use case descriptions, including examples of the use cases in the market, would be beneficial to the FCC as background information. Additionally, areas of concern that did not make the material presented in December also needed to be captured. This would help to assure that the complete landscape of areas of concern found in industry scans and the industry expert discussions were not lost.

This paper contains an expanded version of the "use cases" and "indentified area of concern" sections that are in the main findings paper "**FCC TAC COMMUNICATIONS INFRASTRUCTURE SECURITY WORKING GROUP REPORT: CLOUD SECURITY ANALYSIS AND RECOMMENDATIONS**". It only contains content relevant to mission critical and critical infrastructure use cases and areas of concern.

2. USE CASES

This section contains a more detailed description of the mission critical and critical infrastructure use cases from the working group's main findings paper.

2.1 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

2.2 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 the personnel that maintain the system would need to be vetted against CJIS 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 is an example of this, see CloudLock customer use case.

Instant message and Email services are being hosted in the cloud. There are a number of reports of this use case in the news today. For example, GovPlace reports that government agencies are turning to the cloud to reduce costs of email systems, in their article "Government cloud computing turns to email". Some implementations of these systems will be exposed to CJIS data and are subject to access authorization, encryption requirements, data location, and IT personnel background checks as per CJIS edicts. 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. GCN reports that agencies are considering moving mission-critical applications to the cloud, within the next two years (When NextGen 911 services show up, cloud-based call centers will be ready). These applications include those that access CJIS data, along with storage, records management, crime reporting, and mapping & analysis systems. They reported this as part of the finding from a survey of officials in 272 IACP member agencies. GCN also reports that Durham North Carolina and a few other jurisdictions have already moved their 911 emergency call centers to the cloud.

Municipalities with multiple sites will most likely use the cloud to provide replicates of the data stores at data centers close to branch sites, instead of creating a physical copy of the servers and network infrastructure of the main site local to the branch. This means that in addition to moving application servers to the cloud, the municipality will also rely on the cloud for virtual network infrastructure to recreate municipal sites. In some cases the "headquarters" for the municipality could be entirely cloud based for its application servers and networks as well.

Contact Center solutions that enable managers to view activities in a contact center are moving to the cloud to enable on-demand increased capacity during high volumes. In addition, managers that were tied to their desktops to monitor situations can use the connected anywhere feature of the cloud to walk the contact center floor during a crisis and still monitor call-taker activity. A good example of this scenario is the implementation of a 311 center for any given municipality. Open 311 is an initiative being pursued by cities such as New York, Chicago, San Francisco and Phoenix to provide web based interfaces for citizens to interact with various departments and services. A goal of the Open 311 initiative is to enable incident reporting when full-time call staff cannot be afforded to manage real-time interactions such as phone calls.

2.3 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"

2.4 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 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. This bridge could be dynamic so as to connect the radio systems on demand and disconnect them after the incident has been resolved. Using the cloud to bridge the systems will reduce the cost of implementing these solutions. These links will need to be highly available and secure for public safety needs (this has been referred to as *Interoperability as a Service*). The following article outlines this use case http://fcw.com/articles/2009/04/16/cloud-computing-moving-into-public-safety-realm.aspx.

2.5 PORTABILITY

Municipalities will need the ability to move their applications and data from one vendor to another for a variety of reasons, such as a vendor changing policies or going out of business. The use case described here is a municipality using a secure portable standardized container, such as a virtual machine image, to transfer data and service definitions from one cloud vendor to another. The concern with this use case is the lack of a standard defining a container that is portable between vendors.

2.6 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. Another challenge is the translation of different data formats. Something as innocuous as a phone number may be formatted in one system as 1234567890, whereas another system will need (123)456-7890, requiring software engineers to write custom code--costing time and money.

2.7 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.

3. MISSION CRITICAL AND CRITICAL INFRASTRUCTURE AREAS OF CONCERN

Agencies are currently under pressure from the Office of Management and Budget to identify information technology services that can be moved to the cloud. This pressure is forcing agencies to take steps to ensure due diligence is performed when assessing a cloud providers ability to meet a variety of compliance requirements. 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 had discussions with subject matter experts (SME)s in cloud and hosting technologies. This section takes a look at topics that have bubbled to the surface during our research.

The main areas of concern, along with additional areas of concern, were ranked and are discussed herein. The additional areas are separated from the main list simply to provide some level of stratification to the list. The main areas of concern are top-of-mind for the working group, and the topics also covered in the main Working Group findings paper.

Main areas of concern:

- SLA contract language
- Identity management
- Education
- Cloud certification programs

Additional areas of concern:

- Advanced Persistent Threats
- Privacy and Transparency
- Data classification
- Clean Room Sponsors
- Cloud exit strategies

The following section covers these issues. The concise area of concern in each section is noted by bold font.

3.1 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? Mission Critical and Critical Infrastructure use cases will likely need different service levels than enterprise use cases. Recent articles in the media indicate that any customer of cloud services should look closely at a CSP's SLA to determine if the cloud providers can truly meeting their needs. For instance, this article from Information Weekly points out that an SLA that guaranteed 99.95% uptime did not cover instances of VMs that were sleeping and dependant services that took down the cloud core. Customers were unable to start sleeping VMs during this outage.

There are other articles even more critical of cloud services falling short of SLA promises. Lyida Leong (Gartner analyst) is reported as stating that some SLAs are "practically useless". This reference is gathered from the Network World article Gartner: Amazon, HP cloud SLAs are "practically useless"(December 2012). 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 before mentioned inability to start sleeping VMs combined with dependant 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. There exists a need for a source of information that cloud customers can turn to and get direction on SLA clauses for any cloud service. 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 area of concern. 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 limited to 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. **The area of concern: 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.**

Another alternative to seeking guidance from FedRAMP for local and state agencies is the INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE (IACP). They have issued guidelines for hosting CJIS data in the cloud with the document, "Guiding Principles on Cloud Computing in Law Enforcement". This is document is currently undergoing minor modifications since its initial release in January 2013, but in the end will likely influence requirements for Mission Critical implementations in the cloud.

3.2 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.

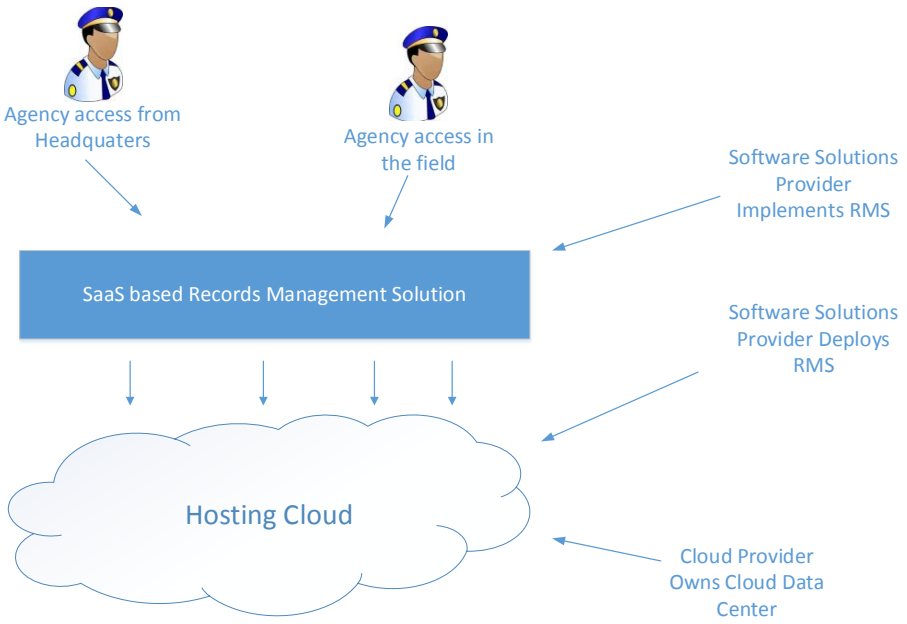
A second area that will present a challenge will be the subject of attribute exchange. Clouds will be required to obtain attributes from a variety of attribute providers in order to make fine grained authorization decisions, and clouds may also be called upon to expose attributes to other clouds. This 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. This is a cumbersome process that no IT administrator is happy with, and often results in stale roles and user permissions being left in the cloud long after a user's roles have changed or they have left the organization all together. 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.

3.3 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.

Let's take for example the security complexities of a SaaS solution for an agency that is provided by a software company deploying a service on top of another company's cloud offering. The diagram below is a very simplified diagram of a Software Solutions Provider with a Records Management Solution (RMS) offering that is cloud based. The SaaS provider offers the solution to agencies that desire moving their solution to the cloud.



In order to understand the potential issues with storing records data in the SaaS solutions, the agency's IT personnel would need to consider, how and where the data was stored, who has logical access to the data, who has physical access to the data, how the data is protected in transit and at rest, how and where backup data is stored, how is the application accessed, where is the application accessed, and how to show chain of custody of the data. This is a daunting task for even the most experienced IT professionals. Now layer on the complexity of understanding security measure of two different companies and we begin to get a picture of the breadth and depth of knowledge needed to create a secure solution.

We have learned, through subject matter experts, 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 aspects 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 as depicted above.**

3.4 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 cloud consumers can turn to for privacy and security assessments. The concern has been easing over the last few years, although it is felt it is not closed completely.

CSA launched the Security, Trust & Assurance Registry (STAR) to help cloud customers understand a CSP's approach to privacy, security and reliability. This program went on-line Q4 of 2011. This program's certification is based on the CSA's Open Certification Framework (OCF). STAR has three different assessments to indicate a CSP's compliance with CSA best practices. For level 1, A CSP can either use The Consensus Assessments Initiative Questionnaire (CAIQ) or the Cloud Controls Matrix (CCM) as evidence of their compliance to CSA's best practices. CSPs may submit their assessment with respect to the CAIQ or CCM to STAR and these reports are published on the STAR Registry. CSA also provides a listing of tool sets that have integrated CAIQ, CCM and other GRC Stack components into their compliance management tools. Though this is not a third party accreditation, it does help cloud customers assess the privacy and security practices and mechanisms put in place by the CSP. For level 2, A CSP can use a third party to show compliance to the aforementioned set of controls. For level 3, the cloud provider can use the continuous monitoring features of OCF.

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 to Operate 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 following are the goals of FedRAMP's 3PAO Program, this taken from their Program Description:

The conformity assessment process is designed to ensure that cloud computing services used by agencies have been assessed by qualified organizations. Specifically, conformity assessment:

- Offers a methodology that allows agencies to ensure that cloud computing services meet Federal security standards for cloud computing systems
- Establishes a standard and consistent security assessment process
- Provides a structure that requires CSPs to use a qualified 3PAO to ensure compliance with FedRAMP and that increases likelihood of a provisional authorization being granted
- Provides CSPs with a framework to integrate with their internal processes and to measure their services against defined standards found at www.FedRAMP.gov
- Provides a scalable framework that can be expanded in the long term, beyond cloud computing.

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 government authorities.** The USDA National Information Technology Center is a FedRAMP compliant CSP and offers FedRAMP-certified cloud services to other federal agencies, as well as to state and local government. Given this example, FedRAMP may be the place to centralize certification for all government cloud usage.

3.5 ADVANCED PERSISTENT THREATS

Advanced Persistent Threats (APTs) are targeted attacks by nation-states, experienced hackers, and cybercriminals that are usually focused on stealing sensitive information from enterprises. These could be general zero-day attacks or ones specifically targeted to your environment. These are difficult attacks to identify using traditional malware detection tools. Traditional tools rely on recognizing a known signature to identify a threat. Zero-day attacks have no known signature until they are found executing in an environment and added to the database of malware in the tool.

Different approaches need to be taken when combating APTs. Prevention techniques include whitelisting, application control via traffic monitoring, behavioral Intrusion Detection and Prevention Systems, and other trusted environment methods such as digitally signed software. These methods have some success in closed environments, but what happens when your neighbor in the cloud becomes infected? Even worse, what happens when your cloud neighbor is the attacker? How can we assure tenants in the cloud are using a minimal amount of protection?

An even greater concern comes into play when the attacker no longer wants to steal data but wants to disrupt services that are a part of Critical Infrastructure (CI). Terrorists are more likely to attack a CI cloud than a social network site. A zero-day virus that could disrupt a cloud that is providing services to utilities for a city could potentially cripple services city wide. **Research needs to be done as to cloud providers' adoption of tools and techniques for identifying and preventing APTs**. At a minimum this would need to be addressed in any SLA with a cloud provider. For example, does a cloud provider have both physical and logical redundancy to combat APTs? What monitoring techniques are being used to identify suspicious application activity?

3.6 DATA CLASSIFICATION

An important step in assessing risk of moving any service into the cloud is to understand and classify any data associated with the cloud service. Consistent data classification between the cloud provider and the data owner is tremendously important to assure both parties are applying the same policies to the data in question. For government agencies, this is crucial when implementing a system that manages data whose access is governed by law. A standard needs to be used by both entities to assure consistency. The standard for classifying government data was established by the E-Government Act of 2002 (Public Law 107-347) Title III, which tasks NIST with responsibilities for standards and guidelines for the classification of data. These recommendations are to be used by all federal agencies to classify their data. NIST's recommendations are documented in FIPS 199 "FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION".

FIPS 199 has been embraced by a key body in the authorization of cloud usage for federal government agencies. This body is the Federal Risk and Authorization Management Program (FedRAMP) within GSA. With respect to data classification, FedRAMP requires cloud service providers (CSP)s to assess themselves against FIPS 199 and present those findings before FedRAMP considers putting them on the list of approved vendors for use by federal agencies. This gives federal agencies some assurances that vendors listed as "Authority To Operate" (ATO) are classifying data in a the same manner as federal agencies. ATO also gives some assurances that vendors follow policies consistent with federal governments when handling their data.

Although this forms a consistent way to classify data for agencies and cloud providers, there are still very few alternatives for cloud providers certified to handle classified data. For instance, the Defense Information Systems Agency (DISA) operates 14 data centers around the world and are looking to be a choice for all government data, classified and unclassified. According to this article, the CIA has been using cloud technology for years. However there is a big difference between privately owned and operated clouds and public clouds. **The area of concern identified here is the low number of cloud vendors that can supply an environment to store classified data.** Even if public cloud vendors would be willing to take on responsibilities for classified data, the real question worth discussion is whether this data should ever be moved to a public cloud, given its sensitive nature. This type of data is likely better served by private or community clouds.

3.7 PRIVACY AND TRANSPARENCY

Privacy and transparency are key concerns when it comes to choosing a CSP to implement a service, especially if the service and its data are considered to be mission critical, business critical or part of critical infrastructure such as public works or utilities. Other data classifications come into play as well when dealing with data being managed by services in the cloud. For instance:

- Is the data a part of public record?
- Is the data government sensitive data?
- Is the data considered "Classified" by the US government?
- Does the data contain PII in it?

Cloud services implementing Critical Infrastructure and Mission Critical applications will be exposed to a set of data that will need to take privacy into consideration. Process transparency will be a key factor in operating a cloud that is trusted by the federal agencies and utility providers. Questions of trust arise around how cloud providers handle data within the data center. For instance, what controls are in place for data that is replicate for geographic redundancy? With services that handle many classifications of data, frequent questions asked by consumers are:

- Where is my data going?
- Who is using my data?
- How is my data being used?
- Who can access it?

In the area of privacy, much government data may not be used for any purpose other than that which is explicitly authorized in writing by the agency that owns the data. This included a popular practice in the cloud environment of mining the data for information that may be advantageous to marketing entities. We would not want car companies mining police report data to find out who has recently had a car stolen to target them for new car purchases. Another scenario we would not want to unfold would be window companies looking for home invasion incidents to target window replacement to victims. Other examples of privacy issues can be derived from "classified" information being leaked to other governments. Privacy is a real concern for data owned and managed by the US Government.

But is there a gap in today's cloud implementations? **There is certainly a perceived gap with respect to transparency and privacy in the cloud environments today**. There are many articles on privacy and transparency that range from opinions to vendor sponsored seminars that discuss privacy. The list below is just a few of them recently found in the media.

- Microsoft sponsored event on privacy, transparency and data protection to increase trust in cloud computing
- Data Guidance reported that the Spanish Data Protection published a guide for cloud providers related to privacy.
- The IT Law Group published Article 29 which is a there viewpoint to risks associated to data privacy in the cloud.

However, the take away from this discussion is that there are places to turn to get some assurances that privacy needs are being met. The answers can be found by using accreditation bodies to gain transparency to cloud

vendor's privacy and security policies and utilities for enforcement. For instance, FedRAMP and the CSA both have accreditation of offerings.

3.8 CLEAN ROOM SPONSORS

Sharing information such as security incidents, latest CERT advisories, and providing threat reports in a non-attributable manner is a cornerstone to protection the nation's critical infrastructure from adversaries. This concern is being addressed thanks to the DHS via a Public-Private Partnerships to Protect Critical Infrastructure and Enhance Resilience, described at http://emilms.fema.gov/IS921/921_Toolkit/downloads/NPPD_Partnerships.pdf.

The National Infrastructure Protection Plan (NIPP) outlines a structure that enables Federal, State, local, tribal, and territorial governments to work with each other and with private-sector owners and operators. The NIPP provides the foundation for a true partnership working to establish national priorities, goals, and requirements; develop joint programs; and communicate and coordinate during incidents.

The Department of Homeland Security promotes public-private partnerships that are the foundation for effective infrastructure protection and resilience. The Office of Infrastructure Protection (IP) supports the NIPP critical infrastructure partnerships and facilitates effective information sharing under the Critical Infrastructure Partnership Advisory Council and the Critical Infrastructure Information Sharing Environment (ISE).

The Critical Infrastructure Partnership Advisory Council (CIPAC) provides a forum for government and critical infrastructure owners/operators to work together to enhance the resilience and protection of our Nation's critical infrastructure. It consists of more than 700 institutional government and private-sector members, including more than 200 trade associations representing corporations of all sizes. A list of all current CIPAC members by critical infrastructure sector is available at http://www.dhs.gov/cipac.

The Critical Infrastructure ISE is a trusted and vetted community of public- and private sector partners who coordinate, collaborate, and share information on critical infrastructure threats, risks, and vulnerabilities. The ISE provides all participants with a unified framework to efficiently exchange critical infrastructure information and conduct incident as well as routine communication and collaboration within each CI sector and across the sectors and geographic spaces. The day-to-day operational sharing of certain critical infrastructure information within the ISE is supported by the Homeland Security Information Network – Critical Sectors (HSIN-CS). HSIN-CS is a secure, unclassified, web-based communications system that serves as the primary, nationwide DHS information-sharing and collaboration system for sharing "Sensitive but Unclassified" information. HSIN-CS supports the ISE by serving as a common platform to provide tactical and planning functionality for private-sector critical infrastructure owners and operators. HSIN-CS participants share suspicious activity reports, incident and pre-incident information, mapping and imagery tools, 24x7 situational awareness, and analysis of terrorist threats, tactics, and weapons.

DHS provides a resource center with detailed overviews, reference documents, and training materials found at http://training.fema.gov/EMIWeb/IS/is860a/CIRC/index.htm.

Private partnerships are also starting to form. One example is Red Sky (http://redskyalliance.org). From their website: "Red Sky offers a confidential environment where companies can share information, learn from each other, compare notes, and be better prepared when hacking comes knocking." They also have a concept called

"Wild Fire" where they call for help on an incident. The collaboration is sometimes used as an out of band war room.

Bottom line – Good progress is being made to enable the MC/CI community to share incident information, with the goal being to strengthen security and protect controlled information on MC/CI computer networks. We continue to study this topic to determine whether this is an actual industry gap.

3.9 CLOUD EXIT STRATEGIES

Agencies need a cloud exit strategy if they want to move their data or change cloud providers. An exit strategy needs to be an integral part of any cloud migration strategy. In https://cloudsecurityalliance.org/media/news/cloud-maturity-study-reveals-top-issues/ by the Cloud Security Alliance, exit strategies were ranked the #2 issue cloud adopters were least confident in. In http://www.cio.com.au/article/423902/cloud_exit_strategy_101/ , cloud security advisor, Rob Livingstone, says that moving into the Cloud is like flying a light aircraft--easy to take off, but a nightmare to land and get out of.

Our research has revealed that while MC/CI cloud adopters are concerned with vendor lock-in when they selecting a particular vendor, there is no clear way to avoid it. Reasons include: as the agency moves to the cloud they are adopting the cloud vendor's security model, data model, backup strategy, and a host of other interfaces. Adding to this is a lack of resources to provide agencies with an exit strategy. There are no clear mandates, instructions, or even checklists on developing a cloud exit strategy.

Some progress is being made toward developing components that work towards an exit strategy. One example is in the Cloud Security Alliance's Portability, Interoperability, and Application Security working group. The working group states, "The concept of portability as it applies to the cloud provides for application and data components to continue to work the same way when moved from one cloud environment to another without having to be changed. Portability is achieved by removing dependencies on the underlying environment. A portable component can be moved easily and reused regardless of the provider, platform, operating system, location, storage or other elements of the surrounding environment."

Some of the Portability, Interoperability, and Application Security working group recommendations include:

- Whenever possible, use virtualization to remove any hardware level concerns.
- If hardware must be addressed, important security considerations make sure that the same or better physical and administrative security controls exist when moving from one provider to another
- Consider using open virtualization formats such as OVF to ensure interoperability
- Avoid service providers that supply services using unpublished "proprietary" APIs
- Understand the size of data sets hosted at a cloud provider. Use interoperable data compression for data moved to and from the cloud to reduce the volume of data being moved and to reduce the time required time to move. Typically there is a cost to move each byte of data into and then, when needed, out of the cloud as well as costs while stored
- Check for compatible database systems and assess conversion requirements if needed
- Make sure security services of your provider adhere to the same regulatory mandates to which you and your data must conform
- Encryption keys should not be turned over to cloud providers

There are also other standards MC/CI agencies must conform to when using a FedRAMP cloud provider including NIST Special Publication 800-88, Guidelines for Media Sanitization and certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."

The FBI's report, "Recommendations for Implementation of Cloud Computing Solutions" talks about CJIS data but only references exit strategy in the context cloud provider ownership change and evaluation of the provider's financial viability. In particular:

- 3.8.1 General: SLA's should clearly identify service provider policy regarding the issues from this section. Contractual agreements should explicitly specify timelines and allowable service changes in the event of ownership transfer of the provider. Discontinuation of cloud services will remain a risk. It is likely infeasible to fully guarantee access to and validation of ancillary and residual data destruction if the cloud service provider discontinues services. The SLAs and contractual agreements should specify the intended actions, and only financially sound providers should be considered. SLAs or contractual agreements should specify service provider responsibilities on the sanitization of data from media and retired devices.

Section 3.8.1 does not make any recommendation or provide guidelines on an exit strategy.

One final note on exit strategies for clouds would be to make conscious and well informed decisions as to how one integrates a cloud into the original environment. Development work may be necessary to create clean interfaces to the cloud in case an exit strategy needs to be implemented. A good exit planning step would be to create well documented interfaces based on standardized APIs to keep rework at a minimum in the process of moving from one cloud provider to another.

As stated above, an exit strategy needs to be an integral part of any cloud migration strategy. This may involve including exit strategy sections in SLA templates for use by entities contemplating cloud adoption.