FEDERAL SUMMITS

FEBRUARY 2017
ATARC FEDERAL CLOUD & DATA CENTER SUMMIT REPORT*

March 29, 2017

Justin F. Brunelle, Sunny Anand, Rick Cagle, Christine Kim,
Michael Kristan, Mari Spina, and Katy Warren
The MITRE Corporation

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

Contents

1 ABSTRACT

The most recent installment of the ATARC Federal Cloud & Data Center Summit, held on February 16, 2017, included five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions. These collaboration sessions allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss challenges the government faces in cloud computing. The goal of these sessions is to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of cloud computing techniques and best practices within the government.

Participants representing government, industry, and academia addressed five challenge areas in federal cloud computing: Developing a roadmap for migrating federal services to the cloud; Securing data in the cloud – Identifying Best Practices and desired outcomes; Cloud services in disconnected and tactical environments; Beyond the Service Level Agreement (SLA): Relationships with Cloud Service Providers (CSPs); and HealthTrac Sponsored Session: Using Cloud in Healthcare.

This white paper summarizes the discussions in the collaboration sessions and presents recommendations for government, academia, and industry while identifying intersecting points among challenge areas. The sessions identified actionable recommendations for the government, academia, and industry which are summarized below:

> As best practices and success stories emerge, government cloud adopters should leverage existing work where appropriate, but maintain agility to refine and customize approaches for their individual needs (e.g., adjusting a cloud migration roadmap).
>
> Industry and government partnerships are beginning to emerge, and government adopters should work *with* industry when designing and acquiring cloud solutions (e.g., security requirements versus SLAs).
>
> Communication, education, and common terminology is paramount in government cloud computing, and government cloud adopters should increase investments in these three areas.

2 INTRODUCTION

During the most recent ATARC Federal Cloud & Data Center Summit, held on February 16, 2017, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in cloud computing. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of cloud computing technologies and research in the government. Participants ranged from the CTO, CEO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs) [7]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology. MITRE works in partnership with ATARC to host these collaborative sessions as part of the ATARC Federal Cloud & Data Center Summit. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in cloud computing, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curricula development, and to help produce graduates ready to join the work force and advance the state of cloud computing research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 COLLABORATION SESSION OVERVIEW

Each of the five MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed:

- Developing a roadmap for migrating federal services to the cloud
- Securing data in the cloud – Identifying Best Practices and desired outcomes
- Cloud services in disconnected and tactical environments

- Beyond the SLA: Relationships with CSPs
- HealthTrac Sponsored Session: Using Cloud in Healthcare

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 Developing a roadmap for migrating federal services to the cloud

The *Developing a roadmap for migrating federal services to the cloud* session focused on the nuances of cloud migration roadmaps that can be reused by government organizations desiring to move legacy systems to a cloud environment. As cloud computing adoption becomes more important, prevalent, and desired, government agencies are migrating legacy services to leverage the benefits of the cloud. However, cloud migration remains a perennial challenge for the federal government. The goal of this session is for participants to establish or recommend a roadmap for migrating legacy services to federal data centers or cloud environments to facilitate future cloud adopters' move to cloud environments. The target outcome of this session is a series of steps, potential pitfalls, and a general plan for cloud migration.

This session had three goals:

- Identify general process for cloud migration;
- Identify potential pitfalls or challenges; and
- Document success stories and recommended methods to overcome challenges

with the goal of producing high-level roadmap for future government agencies to use when migrating legacy services to a cloud environment.

Diversity among the participants in this session in business domains, cultural norms, and levels of cloud architecture and implementation experience made for a dynamic conversation. However, this same breadth of engagement also exposed challenges with audience agreement upon a single, universally reusable roadmap for future government agencies to follow. Rather than accept stalemate on reaching consensus on one path for all to follow, the session labored instead toward laying out a cloud geography, populated by recognized landmarks, milestones, and potential hazards. Participants concluded that plotting an appropriate course, and navigating this terrain, is in the purview for each organization on its journey to cloud solutions, with a framework suggested by the session for how an organization should develop its roadmap.

3.1.1 Challenges

The session opened with brief introductions to acquaint participants, and as part of introducing themselves, each was invited to include a few words on concerns driving attendance at this discussion. Concerns were as diverse as the audience, ranging from high-level and more general, to quite specific and granular. Where duplicate items were identified, they were refined to aggregate by repeated emphasis and allow for subtleties of distinction. They were then weighted to help prioritize how to best use the time and work toward the session goals, while accommodating as much of the audience as possible in the venue.

Many in the audience were cloud novices at best and had come to listen, ask questions, and learn. They represented categories structured around "how to migrate to the cloud" and focused on understanding and developing a workable shared vocabulary. Issues introduced included "What does 'roadmap' really mean in a cloud context?", "Who owns the roadmap?", and "Who should even be able to access it?". Others were further along in their cloud migration activities, bringing with them into the conversation more detailed concerns targeted to specific areas of business challenges or architectural considerations. These included areas usually well explored in the IT domain, but presenting unique aspects due to the influence of the cloud; such as how to embed security into the process, what portability and vendor lock-in concerns exist, or how to tool properly based on the resulting roadmap.

Many of the drivers discussed were parallel to the set produced by the July 2016 ATARC Federal Cloud Summit session on Cloud Category Management [2], underscoring the persistence of those themes. Some concerns were broader, but still affected by new patterns to be applied because of application to the cloud environment. These included how to address economics, such as for acquisition and procurement management when shifting from a model of capital expenditure to one centered on operational expenditure. A good many were interested in establishing parameters to measure costs, plan budgets, and determine return on investment (ROI) or conduct Analyses of Alternatives in a cloud context. Still others wanted to explore effects of cloud interactions with other recent or emerging concepts, such as Agile and DevOps.

Finally, a few present could be said to be comparatively advanced, and had much to offer the first two groups, from a post-roadmap perspective, on "gotchas" or lessons learned from crafting and following a roadmap to their cloud migrations. These thought-leaders had collected experience along their way to realizing cloud ambitions, and were busy refining and perfecting, and were looking to learn from peers who had reached a similar level of maturity in thinking and process. They brought with them forensic considerations for many of the new and intermediate areas of questions, such as how to engage people in the stewardship of

the roadmap and partnership in the migration.

The collaboration session discussions identified the following challenges that might be solved and needs that might be met by applying existing or developing new *Developing a roadmap for migrating federal services to the cloud*:

- Why are you going to cloud? How do you set the vision to guide and constrain the roadmap?
  - What are the benefits of going to the cloud?
  - What are your drivers?
    - What are you moving?
    - Who are your *Sherpas*?
    - What are risks? What is the best mitigate strategy?
    - What are your constraints (including people)?
  - What are your risks?
  - What is your timeline?
- On what factors should you base your assessment?
  - What are your metrics and success factors?
  - Who are your stakeholders?
  - How do you define way-points, milestones, and landmarks around which to construct a roadmap?
- How do you integrate the different perspectives of stakeholders in the roadmap?
  - Business
  - Technical
  - Others (Where am "I" on the roadmap? What do "I" need?)

3.1.2 Discussion Summary

The following two items were among the most actively discussed in this context:

- What are considerations for Cloud Roadmaps?
- What are the "Gotchas"? What are "Lessons Learned"?

With respect to the most discussed topic, “What are considerations for Cloud Roadmaps?”, the audience breadth and diversity was put to perhaps its best advantage. The different levels of experience, varied business domains, and distinctive cultures and engineering challenges each constituted enabled the group to provide the best input on addressing the landscape of issues and obstacles, opportunities and risks. This included those areas of concern most impacted by cloud qualities, which they had either already overcome, or with which they were currently wrestling. The collection the group identified and felt were most impacted by introducing cloud were:

- Identity Access Management
- Licensing
- Performance
- Network Connectivity
- Deployment
- Data Location
- Data Conditioning Services
- Refactoring
- Logging & Auditing
- Availability
- Disaster Recovery & COOP
- Automation
- Analytics
- Administrative (Costs, Management, Pricing, Budget)
- How do you include DevOps?
- SLAs & Quality of Service (QoS)
- Governance?

- Diversity (multi-cloud topologies)

The audience dialogues were quite productive, and often demonstrated the value of this type of forum, with mutual learning opportunities, and sharing of knowledge openly, from the array of backgrounds. A smaller, but important section of the conversation evolved beyond the roadmap debate, and the resulting accord on understanding of the cloud migration geography as a step toward properly establishing roadmaps. Namely, how the groups could benefit from many of the hard-won struggles of the more advanced participants in defining, documenting, and executing against the roadmaps that had gotten them to the cloud. This sharing included lessons learned by those who were further along in their cloud journey, and examples of "gotchas" encountered along the way.

It was agreed by all that "cloud" itself is so laden with buzz-words, vague definitions casually used, and wildly varying levels of hands-on experience, a solid grounding in standards such as those produced by National Institute for Standards and Technology (NIST) for cloud terms, reference architecture, services and deployment models is a critical best practice for surviving, let alone driving a migration. Organizations should develop a Concept of Operations (CONOPS) for a clear understanding of how cloud is to be applied for their situation and to address their business, technical, and operational needs.

The introduction of cloud into the IT ecosystem has profound impacts, starting with acquisition planning and shifts from a Capital Expenditure (CAPEX) to an Operational Expenditure (OPEX) mind-set. It continues through the development lifecycle of any software in a cloud-native environment, impacting talent acquisition and development, support and contractor qualifications, involves trouble-shooting potentially shattering many traditional boundaries, and introducing and enriching many new feedback loops. Operational issues expand, introducing bandwidth challenges for access and performance, and entirely new classes of security threats.

3.1.3 Recommendations

The participants in the *Developing a roadmap for migrating federal services to the cloud* collaboration session identified the below important findings and recommendations.

Develop customized roadmaps.

There may be no single cloud roadmap, generic enough to apply to the vast assortment of differing needs, but still specific enough to supply practical guidance for migration to the cloud. It is recommended that organizations construct a roadmap suitable to their circumstances, guided and constrained by considerations presented in this session.

Consider the similarities to a geographical map, which scopes itself to a certain area, identifies boundaries, landmarks, obstacles, hazards, and other navigational information the reader needs to analyze any number of possible routes to reach a destination. This map enables the reader to then make the best decisions in planning how to traverse the distance, given the circumstances of travel, traffic, and other conditions impact them as they travel toward their destination. This same map can be used to manage unforeseen conditions arising during travel, forcing deviation from the route originally planned, and to make corrections as needed to avoid unfortunate developments, or to take advantage of emergent opportunities. The map is a framework, and the route actually travelled is based on decisions at the time of planning, as well as reactions to developments in pursuit of the destination.

Likewise, the work accomplished by participants in this session represents the best cloud cartography synthesized from those who have navigated routes across this landscape. This framework was then examined, challenged, refined, and agreed upon by a broad representation of academia, industry, and government, all engaged in diverse efforts to move enterprises across this terrain. Some present had made significant progress toward a destination, with stories of re-planning and responding along the way; others were just starting out, and interested in reports from those ahead on changing conditions, and obstacles perhaps not indicated on the maps they'd drawn; and still others uncertain of how – or even whether – to begin at all.

Communicate and learn from peers.

Considering the productivity in the conversation, and the open sharing and learning that many in the session enjoyed, it is recommended to continue the forum for interaction, where participants can so learn from each other. GSA, for example, hosts a site and regular meeting forum for Cloud Access for Federal Enterprise (CAFE)[1], which is an initiative to simplify cloud acquisition in government. Broader treatment, such as a government-wide, industry and academia-supported Center of Excellence would expand the focus beyond CAFE's narrower purview, and provide a construct to continue the accomplishments of this session. Workshops for future ATARC sessions could help to seed such efforts, with goals of developing the roadmap framework suggested by this session. Another candidate for a future session could include development of a similar framework for organizations to tackle CONOPS for cloud specific to their business domain and technical requirements. A format building upon the success of the discussion in this session, modeled after the CAFE structure, and expanded to include development and execution of organizations, programs,

[1] `https://interact.gsa.gov/group/CAFE`

and projects embracing cloud would be a cornerstone of any Center of Excellence formation.

Summary

This session built upon the foundation laid in the January 2016 session on Planning for Cloud Migration and key elements from the July 2016 session on Cloud Category Management. The more than seventy participants ranged in level of experience with Cloud Migration from curious learner to confident implementer, and brought a variety of perspectives to the conversation, including technical, business domain, organizational culture, and policy views. With such diversity, the progress made toward a reusable roadmap included primarily nominating, describing, debating, refining, and documenting common, if not universal milestones. Participants worked throughout the session to categorize these "waypoints" broadly as common core components, best practices, or risks and lessons learned. Members worked to associate these in a framework for constraining and shaping Cloud Migrations. It was conceded that across this Cloud Migration terrain likely lie many possible paths to success. Organizations must provision and implement a roadmap using such a framework, driven by specific requirements of the organization's domain, culture, and project. Orienting migration planning with respect to these points, and navigating toward an organization's cloud goals will require constructing a suitable roadmap from a framework further developed from the work began by the participants was the key accomplishments of the session.

3.2 Securing data in the cloud – Identifying Best Practices and desired outcomes

The *Securing data in the cloud – Identifying Best Practices and desired outcomes* session focused on specific challenges related to delivering security to deployed cloud systems and data (i.e., the security of systems, data, and processes within a cloud environment as opposed to securing access points to clouds or the internet).

Participants to the session were asked to share their security challenges and to offer solution options and associated personal experience in response. Consistent with the July 2016 Cloud Summit recommendation for agencies to take ownership of cloud security [2], participants were truly interested in finding solutions to baking security into their cloud system deployments rather than relying on cloud service providers.

From the session, it was clear that security remains a primary concern when using cloud services in a government agency. As such, group discussions covered a broad range of topics including organizational change for cloud adoption, acquisition practices for proper contracting, and the technical details of implementing cloud security solutions.

This session had two goals:

- Discuss challenges with CSP-provided storage and data security and
- Identify best practices for agencies when storing data

with the goal of producing recommendations for agencies to take ownership of data protection in a cloud environment.

3.2.1 Challenges

Session discussions identified a number of interesting challenges. Topics included a mix of technical, operational, and organizational issues. Participants expressed associated challenges related to:

- Securing the Virtual Machine (VM)
- Securing Interfaces to CSP systems such as Application Program Interfaces (APIs) and micro-services
- Preventing bridging across multiple authorized cloud connections within a single agency network
- Responding to data spillage in the shared operational environment of the cloud; What can we ask of the CSP?
- Executing continuous monitoring for threat mitigation and compliance; Is the data sufficient?
- Methods for encryption key management
- Collaboration between IT and Acquisition departments to ensure security is baked into contracts
- Obtaining a Cloud Security Reference Architecture to guide security solutions
- Understanding the CSP's authorization boundary in the event of new service delivery; does a new service affect the FedRAMP [6] Provisional Authorization (PA)[2]?

[2]More information on FedRAMP PA at `https://www.fedramp.gov/resources/faqs/what-is-a-fedramp-provisional-authorization/`.

3.2.2 Discussion Summary

There were many excellent solutions and personal experience stories brought by participants to address the challenges expressed. And again, solution options and experience stores centered upon cloud security technology, operations management, and associated organizational factors.

From the technical perspective, technology considerations involved selecting the correct service model, securing communication channels, and employing the NIST virtualization security practices [3]. It was noted that private clouds are preferred over community and public clouds when strict VM isolation is desired. The Azure Government cloud was mentioned as a commercial cloud option for specifically handling International Traffic in Arms Regulations (ITAR).

Use of network segmentation tools offered by the CSP such as the Amazon Web Services (AWS) Security Groups and Access Control Lists (ACLs) [1] was offered as a best practice. For additional enclave security, it was noted that network firewalls, Web Application Firewalls (WAF), host based intrusion detection tools such as those offered by the McAfee ePolicy Orchestrator[3] (ePO) and Host Intrusion Prevention System (HIPS)[4] could be brought to bear in an Infrastructure-as-a-Service (IaaS) service model.

Use of Internet Protocol Security (IPSEC) Virtual Private Networks (VPNs) and the CSP's direct connection capabilities, where available, were offered as best practice solutions for connecting the agency network to a CSP for intranet and/or management networking purposes. For use cases involving the use of multiple connected clouds, it was suggested that a Cloud Access Security Broker (CASB) may be useful. This is a relatively new concept introduced by the Gartner Group in 2014 [4]. These 3rd-party providers can deliver identity federation, secure connectivity, and agency network boundary security-as-a-service. CISCO Cloud Lock[5] and Sky High Networks[6] were noted examples of CASBs.

To secure interfaces to the CSP's systems and services, use of mutual authentication TLS/SSL was offered as an effective best practice. Use of 3rd-Party API Gateways (GWs), designed to mediate traffic flows was further suggested.

On the topic of data encryption key management, it was noted that while CSP offered Key Management Services (KMS) could be an effective means for creating and managing encryption keys, use of a CSP's FIPS 140-2 compliant Hardware Security Module (HSM)

[3] https://en.wikipedia.org/wiki/McAfee
[4] https://en.wikipedia.org/wiki/Host_Intrusion_Prevention_System
[5] https://get.cloudlock.com/
[6] https://www.skyhighnetworks.com/

should be employed when storing keys in the cloud. However, a few participants noted that many of these services had not been authorized under CSP FedRAMP PAs.

On the topic of FedRAMP PAs, some participants expressed concern with the FedRAMP authorization process and in its ability to assess CSP compliance when new services are offered before they are accredited or are not slated for assessment. The concern is that related underlying systems may operate within the CSP's authorized accreditation boundary and therefore impact the original PA. This is not a question the group was able to answer.

From the operational perspective, cybersecurity operations management discussions centered upon use of an array of tools including contractual terms and conditions, SLAs and operational level agreements (OLAs). It was noted that the FedRAMP web site provides an excellent source for standard cloud service contracting clauses.

From a development-operations (DevOps) perspective, participants indicated success when applying a CSP's deployment templating or quick start system for enforcing configuration policy in system deployments. However, participants noted that deployments could only be successful if cloud security event and incident systems warning systems could be integrated with existing enterprise security information and event management (SIEM) systems and compliance monitoring systems. This is where lack of an agency cloud security reference architecture caused the greatest pain.

Finally, the group indicated that federal agencies continue to be plagued with IT skill deficiencies and noted that they are most evident in the procurement offices. Siloes may persist that inhibit the infusion of IT talent into the procurement agent ranks. Some of this could be due to the fact that cloud technologies and service offerings are relatively new and are constantly evolving.

3.2.3 Recommendations

The participants in the *Securing data in the cloud – Identifying Best Practices and desired outcomes* collaboration session identified some very interesting challenges that appear to be consistent with the maturity in the adoption cycle. As government organizations have forged ground in the cloud, we are seeing levels of knowledge go up and challenges getting deeper into the details. From this perspective, we are making great progress as a community but improvement is certainly needed. Findings and recommendations:

- Cloud technologies and service offering are evolving quickly and maintaining or improving the agency security posture remains a key factor in cloud adoption. In this regard, continued discussion and sharing of best practice options and solutions within

the community must continue.

- CSP security systems and solutions are a valuable tool for agency security operations but the lack of integration with existing agency cyber defense systems hinders successful cloud-based cyber security operations. Accordingly, Agencies are urged to develop their own Cloud Security Reference Architectures to address cyber security systems and integration concepts.

- The "rubber hits the road" when federal agencies contract for cloud services but many agencies are feeling inadequately armed with necessary IT skills to address cyber security in procurements. Accordingly, agencies are urged to seek improved integration between IT Service Delivery, Security Operations, and Procurement Departments.

3.3 Cloud services in disconnected and tactical environments

The *Cloud Services in Disconnected and Tactical Environment* session recognizes that cloud environments are uncommon in disconnected environments, whether they be cloud nodes in a tactical battlefield environment or end user devices trying to access a centralized cloud from a location without cellular or data access. However, government cloud adopters are working to establish cloud environments and access patterns from these disconnected environments, including edge devices termed cloudlets that can perform limited cloud functions at the tactical edge. This section discusses current efforts, recommendations, and provide guidelines for future tactical cloud efforts within the government.

Participation included individuals from non-government organizations (NGOs), military, and civilian agencies. Use cases identified for this discussion included a disaster response scenario with a mobile command system such that severed communication creates a closed network. Another use was an application like an email client with the ability to have an offline mode. Stateless applications with cached data sets such as a localized language translator, and a fleet of connect edge devices that bring content as close to the end user as possible, like a home cable television unit that caches on-demand movies.

For the purposes of the discussion group, a reference architecture was crafted. Figure 1 illustrates three distinct classes of systems. Starting from the right is a traditional enterprise cloud environment. In the middle is a potential edge or tactical cloud. Finally, on the left is a set of clients which may connect to the tactical cloud. The communications between each of these devices will vary or may not exist at all. Data may or may not be persisted on the tactical cloud or edge device.

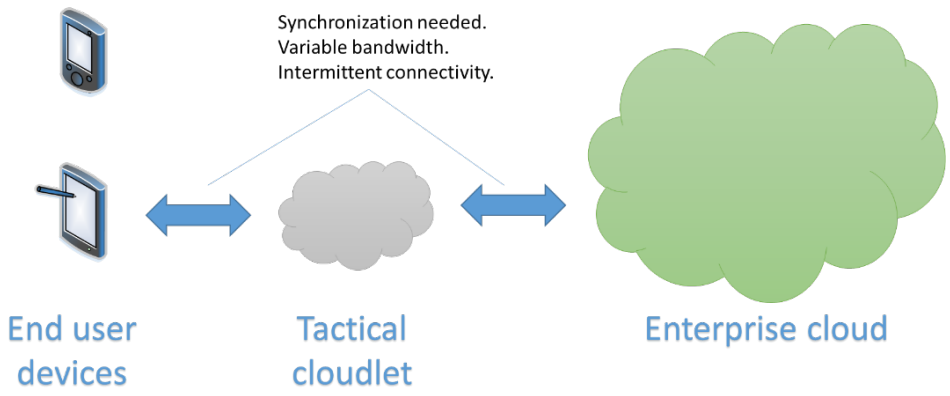

Figure 1: A system diagram illustrating the relationship between end users, cloudlets, and enterprise clouds.

This session had three goals:

- Discuss common criteria that create a disconnected or tactical cloud environment;
- Discuss the current tactical cloud solution space; and
- Provide recommendations for future tactical cloud research

with the goal of providing documented recommendations for future tactical cloud development, adoption, and research to help close capability gaps.

3.3.1 Challenges

Disconnection can be deliberate or unpredictable and the disconnection can be short term or long term. It is also important to point out that in a tactical environment, degraded communication is possible where the link may be slow or error-prone. Regardless, the primary purpose of these cloud services is the ability to service on-demand requests. The participants identified many challenges when users are attempting to access cloud services in a disconnected space.

- Applications that are not developed to operate in partially disconnected or fully disconnected environments without broad reach back
- Large data requirements at the end of smaller or non-existent communication links
- Synchronization and replication of data to the tactical edge

- Security boundaries or intentional air-gapped clouds due to requirements
- Continuous monitoring of the edge devices
- At rest encryption and key management of data in cloudlets
- Authentication and authorization when identity providers are not synchronized to a master data store
- Procurement and acquisition

3.3.2 Discussion Summary

Security topics were the most actively discussed items although other items such as scaling and replication were discussed. Security topics included data security, attack vectors, tenancy, and identity management. The team identified that with a cloudlet on the move, the physical security practices differ. For example, how does one protect data if the cloudlet is highjacked or moved to an area where the data is not allowed to go (e.g., violation of export controls by moving to a geographic area)? The communications links need to be secure to prevent man-in-the middle attacks. The overall trend was to limit the amount of persisted data on the cloudlet and end user devices whenever possible as length of storage may define security risk. Therefore, treating the end user devices as thin client is preferred. To address the tenancy issue, the recommendation was to use single purpose containers that are compact. The value of containers with appropriate logical separation will allow for isolation of data sets.

Identity, authentication, and authorization were important topics. In a disconnected environment, pre-provisioned credentials are inevitable [5]. Synchronization and revocation of credentials may be done out of band if the disconnected environment is away for a long period. Multi-factor and biometric authentication mechanisms were discussed as possible identity sources. Another question that was discussed included making authentication decisions based on connectivity (for example in a disconnected state not having full sets of permissions). As the Internet of Things (IoT) becomes more common in a tactical environment, solving the authentication and authorization challenge become more important.

At the end, scaling and replication were discussed. As demand increases and one needs to take advantage of the elasticity of cloud, the idea of scaling comes in to mind. One scenario is adding more cloudlets to the tactical edge and removing cloudlets when the demand changes. Replication and management become issues. Related to scaling is the idea of

making cloudlets generic in nature so to avoid vendor lock in. This creates interoperability challenges and will need to be explored.

3.3.3 Recommendations

The participants in the *Cloud services in disconnected and tactical environments* collaboration session identified the following important findings and recommendations:

- Define a suitable CONOPS for disconnected clouds to which a pilot can be developed
- When deploying an operating a disconnected cloud, do so with the assumption that an IT expert will not be able to directly service devices and links
- Design a disconnected cloud environment with flexibility in mind
- Add cloudlets and end user devices to accreditation policy and consider constant re-accreditation
- Consider scaling challenges at the edge to include load balancing and loss of efficiencies of scale because of the need to manage multiple clouds

3.4 Beyond the SLA: Relationships with CSPs

The *Beyond the SLA: Relationships with CSPs* session focused on improving services available to government cloud adopters without relying strictly on paperwork agreements. Traditionally, risk management, roles, and other aspects of cloud DevOps has been managed through custom SLAs. While this is a reasonable approach, this session's goal is to identify ways to work with commercial CSPs to improve service offerings, improve portability, or make migration easier. This may include discussions regarding vendor lock-in or DevOps ownership, and should discuss services from cloud brokers or CSPs that can help the government improve its cloud usage.

This session had three goals:

- Discuss current incompatible practices by government cloud adopters and CSPs;
- Identify useful services that will improve government cloud adoption; and
- Discuss the ownership of DevOps practices, and how ownership of DevOps can improve cloud migration and usage

with the primary goal to identify best-case service offerings from CSPs as a way to encourage CSP-provided service for government consumers.

3.4.1 Challenges

The collaboration session discussions identified the following challenges with developing SLAs between government cloud adopters and CSPs:

- Creating SLA standards and guidance that works for both agencies and CSPs
- Finding an effective way to measure standard
- Sharing roles and responsibilities of an SLA efficiently
- Enforcing the SLA as both the CSP and the customer (i.e., government agency)
- Making an SLA that is manageable and not overwhelming
- Keeping up with the rate of innovation and new technology advances for cloud
- Developing and maintaining transparency in cloud operations for all stakeholders

3.4.2 Discussion Summary

The discussions in this collaboration session varied but had four common themes: SLA standards and guidance, Roles and responsibilities in SLAs, SLA enforcement, and Communication for SLAs. We provide a summary of the discussions according to these themes.

SLA Standards and Guidance; Agencies vs CSPs

A primary topic of conversation was creating standardized, repeatable SLA's – or SLA templates – that are useful across a broad spectrum of government organizations and missions. Frederic de Vaulx, the government session lead from NIST, explained how NIST has been working on establishing an SLA framework composed of a set of building blocks, that can be used as SLA topic areas (such as performance, security, monitoring, and enforcement) including guidance for measuring compliance with the SLAs. The goal is to create a framework for SLA development available to all agencies.

Roles and Responsibilities in SLAs

Shared responsibilities and roles should be described in the SLA. Since the cloud integrates a significant number of different components, it is very difficult to determine what and where things go wrong within the cloud. Many are struggling to construct an SLA between several individual parties, which has forced all cloud and service providers to – as of now – simply get used to working together to provide a cloud service.

"What if" SLA Measurement and Enforcement

Some government representatives voiced concerns regarding current SLA management. For

example, the possibility of signing up for a bad SLA. There are cases where an SLA can be written very well, but execution is poor; the alternative can occur where an SLA is written poorly but executed well. An SLA must be carefully written and monitored to ensure that it is neither too vague (causing the product to be different than what was intended) or too specific (allowing for pigeon-holing the product into something that was also not wanted).

SLA enforcement and penalties received significant attention in the discussion. Some vendors have pre-established SLAs, potentially approved via FedRAMP, that can be difficult to modify. However, SLAs may be negotiated between parties whereby specific criteria are established. An incentive based approach could be very effective in many cases. It is important to consider multiple methods in developing the best usage of an SLA.

Communication for SLAs

Relationships and communications between the government and the cloud service providers is key in general operations and resolving problems. By having a trusting relationship and environment, the creation and enforcement of the SLA is more effective. An SLA does not only exist for enforcement, but also for communication. It is evident that different parties will have different goals, such as profits or missions, but an SLA will be effectively able to establish the basis for mutually achieving the goals of all parties.

3.4.3 Recommendations

The participants in the *Beyond the SLA: Relationships with CSPs* collaboration session identified the following important findings and recommendations:

- ***Remain outcome-based.*** Measurement of the metrics and outcomes of an SLA will ensure that there are clear guidelines being written.
- ***Define shared responsibilities.*** By specifically defining the shared responsibilities, there will be less difficulty in the future with finding what came from where within the cloud (i.e., this helps to establish costs and penalties for any issues).
- ***Maintain communication.*** Having a trusting relationship filled with effective communication between all parties involved in the cloud service will help to make the SLA more effective.
- ***Invest in industry cloud education.*** Defining *cloud* and educating all parties on common terms will make sure that people will be signing up for what they actually want on the SLA.

- ***Incrementally improve on a generic framework.*** An SLA can become more effective in the future with the use of a developed generic framework. Incremental changes can then be made to this framework based on the given scenario.
- ***Establish a common vocabulary.*** Using common language that will become recognizable to all parties (including both the provider and the customer) will help with communication of the SLA.

3.5 HealthTrac Sponsored Session: Using Cloud in Healthcare

The *HealthTrac Sponsored Session: Using Cloud in Healthcare* session focused on healthcare challenges in the cloud, and specific aspects of cloud computing that make healthcare, in particular difficult. In only a few short years, cloud computing has altered the information technology landscape – yet the digital transformation is only beginning, especially for DoD, Veteran's Affairs (VA), and other Government Healthcare Agencies. Cloud computing is not a matter of *if*, it is a matter of *how* and *where*. Government Healthcare Agencies need to balance the benefits from accessibility via the cloud with the risks created by increased accessibility. This session will focus on tackling the following key questions around:

- Cloud Computing Environments,
- Security & Privacy, and
- Governance.

This session's goals and activities are defined by the VA Interprogram Office (IPO) with MITRE guidance. This session had three goals:

- Discuss appropriate *cloud computing environments* to transform application delivery to support business agility;
- Explore steps that government healthcare organizations should take to protect the *security & privacy* of health information data; and
- Collaborate on achieving the ideal *governance* mechanisms whereby a level of control is transferred to external parties responsible for delivering IT services.

3.5.1 Challenges

The collaboration session discussions identified the following challenges that might be solved and needs that might be met by applying existing or developing new *HealthTrac Sponsored Session: Using Cloud in Healthcare*:

Cloud Computing Environments

- Which is the right choice?
- How do I start?
- How to transform my application delivery to support business agility?

Security & Privacy

Healthcare information is valuable; for example, a health record is estimated as 10 times more valuable than a credit card record to cyber thieves. What steps should government healthcare organizations take to protect health information, while benefiting from the increased availability with cloud computing?

Governance

Cloud computing creates a paradigm shift for delivering IT services, whereby a level of control is transferred to an external party. What policies and procedures enable healthcare organizations to protect health information systems partly controlled by an external party, while improving agility?

3.5.2 Discussion Summary

The items in this section were among the most actively discussed by the session participants.

Cloud Computing Environments

How should Government Healthcare Agencies deal with a moving industry? Individual agencies have their own policies and thresholds to handle sensitive data. For example, VA may be more flexible compared to DoD with having health data on smart watches.

Security & Privacy

There is a legal aspect to where the information resides.

- How is record validation carried out?
- How you leverage data in stores that can be standardized?

Eliminating the need for SSN as a unique identifier contradicts DoD ID (DIN number) in the cloud. The main purpose is providing healthcare by putting in electronic healthcare

records (EHR) systems in place. However, if private medical practitioners share their data, they give away their business. There are bad elements who steal health info to misuse it. Cases were cited of selling cancer patients records and use insurance malpractices to get treatment.

Governance

It is a shared responsibility. Questions that arise surround concerns around the question of *Who owns the data? Who is empowered?* There are concerns over data sensitivity levels – HIPAA vs. FISMA High. Overlaps exist between the two compliance efforts, but there are also contrasting objectives in following these compliance regulations. There was a notion to extend Privacy (HIPPA & Business Associate Agreements).

Concerns surrounding data storage and records management surfaced. One of the participants voiced that data will have to exist for 125 years. There are a limited number of vendors in healthcare space – only three authorized cloud providers for health care (i.e. AWS, Microsoft, and CSRA).

3.5.3 Recommendations

The participants in the *HealthTrac Sponsored Session: Using Cloud in Healthcare* collaboration session identified the following important findings and recommendations:

Cloud Computing Environments

One of the ways to stay abreast in a moving industry is to look at direction where rest of the world is looking at. Participants identified a need to define a leapfrog business model that would inject medicine and provide predictive analytics using digital analytics and IoT for a well-rounded perspective. For a more impactful healthcare, the medical doctors workload needs to be lessened. Since time is of essence, let them use 15 minutes for quick decisions without human risk.

Security & Privacy

Cloud, or even the technology, doesn't fix the challenges outlined in this section. Participants in the session identified the need for a new business and operations model with DoD and VA communities. There is a need to define business functions and then come up with an operating model that characterizes the business model. Handling all medical information through Levels of Assurance (LoA) coupled with FISMA - High are a step towards assessing risks associated with electronic authentication and identity proofing.

Discussions converged on questioning the benefits of cloud computing. The security aspect (i.e., access) could be improved with biometrics. Extending that thought, access management could be fortified by securing mobile devices. Typical implementation concerns

that agencies must address in their Security Plan should include:

- Incident response capabilities (shared responsibility)
- Identity & Access management
- Multi-factor Authentication
- Trusted internet connection (TIC)
- Continuous Monitoring
- Securing end devices

Governance
Participants identified the need for an operational model that looks at data integration with personally identifiable information (PII), health information databases, and statics driven data engines. They looked at modeling "single source of truth" with a validated model that uses calibrated medical devices, provider notes/opinions that are "signed, sealed, and delivered".

Entities like Office of the National Coordinator for Health Information Technology (ONC) helps set the standards towards achieving common source of truth. Genetics driven data models can showcase behaviors for preventing population health problems.

The strategy for acquiring cloud services should encompass:

- Policy Considerations,
- Service Level Agreements, and
- Exit Strategy.

4 SUMMIT RECOMMENDATIONS

During this instalment of the ATARC Federal Cloud & Data Center Summit– as with past summits – the participants and their discussions provided a subsample of the state of cloud computing in the federal government today. While the specific challenge spaces provide their own themes, challenges, and recommendations, several overarching themes provide insight into the state of the discipline of cloud computing in the government.

Primarily, we are seeing *cloud champions* emerge in the government; in other words, individuals working within the government are working to make cloud adoption more effective

and easier for new adopters. To that end, we are seeing best practices emerge for developing cloud roadmaps, security, SLAs, etc. However, despite some common elements and common recommended best practices, government adopters should initially adopt existing successful methods, but should revisit these practices to refine and customize their use of the methods to better serve their specific needs. Even in the specific use case and domain of tactical and disconnected cloud environments, the ability to be flexible, adaptable, and scalable was identified as a primary recommendation.

Participants also acknowledged that some metrics that have traditionally been used to measure government cloud effectiveness (including those in SLAs) are becoming archaic (e.g., uptime). Instead, the participants recommend focusing on metrics that evaluate outcomes, levels of service, and are adaptable to innovation and evolution of cloud services. Similarly, the migration roadmap and security sessions identified similar needs to focus on outcomes rather than methodologies.

Cloud is still an emerging discipline in the government healthcare domain and – as such – is wrestling with the perennial challenges in cloud computing (e.g., privacy, cost, acquisition). Despite these common challenges across other disciplines of cloud adopters, cloud adopters in healthcare cite very specific use cases and end states that they are trying to achieve (e.g., using cloud services to better diagnose patients). The healthcare domain can greatly benefit from the use of cloud services and is expected to resolve its current adoption challenges by leveraging and adapting existing practices.

As is always recommended by participants, communication and collaboration between agencies and industry, government, and academia is key to the success of cloud computing in the government. As such, events like the Federal Technology Summit Series will increase in importance for technology adopters.

5 CONCLUSIONS

The February 2017 ATARC Federal Cloud & Data Center Summit highlighted several challenges facing the Federal Government's adoption of cloud computing.

- Cloud migration roadmaps may vary, but have common "waypoints" along the path of adopting cloud services.
- Security – still a primary challenge and concern in cloud – has benefited from defined architectures and best practices.

- Previous edge cases in cloud computing (e.g., tactical clouds) are becoming more common place and are providing beneficial research that improves traditional cloud paradigms.
- SLAs are moving from metric-based to outcome-based and are improving due to collaboration between government and industry.
- Healthcare is continuing to evolve and refine their approach to addressing the perennial cloud computing challenges.

While the February 2017 ATARC Federal Cloud & Data Center Summit highlighted areas of continued challenges and barriers to adoption, the Summit also cited notable advances in mitigating these perennial challenges. While security, service level agreements, and migration remain primary challenges, recommendations and roadmaps for mitigating these challenges are emerging.

Based on the recommendations made in the Collaboration Sessions, government practitioners (at all levels of government) should participate in special interest groups or working groups to increase collaboration; continue to influence standards development within the discipline; and continue to partner with academia to leverage cross-cutting research and to help train the government workforce. Including academics in the research process can help provide solutions to challenges that are not currently financially appealing to commercial vendors. These activities will further mitigate the perennial cloud adoption challenges cited by the participating cloud practitioners.

ACKNOWLEDGMENTS

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit.

The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the FedSummits web site[7].

[7] http://www.fedsummits.com/cloud/

REFERENCES

[1] Amazon Web Services. Security Groups for Your VPC. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html, 2017.

[2] J. F. Brunelle, D. Davis, N. Gong, D. Huynh, M. Kristan, M. Malayanur, T. Harvey, and T. Suder. July 2016 atarc federal cloud computing summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[3] K. Dempsey, N. S. Chawla, A. Johnson, R. Johnston, A. C. Jones, A. Orebaugh, M. Scholl, and K. Stine. Information security continuous monitoring for federal information systems and organizations. Technical Report Special Publication 800-137, National Institute of Standards and Technology, 2011.

[4] S. Deshpande, N. MacDonald, and C. Lawson. Emerging Technology Analysis: Cloud Access Security Brokers. Technical Report G00264199, Gartner, 2014.

[5] S. EcheverrÃŋa, D. Klinedinst, K. Williams, and G. A. Lewis. Establishing trusted identities in disconnected edge environments. In *2016 IEEE/ACM Symposium on Edge Computing (SEC)*, pages 51–63, 2016.

[6] FedRAMP PMO. FedRAMP. https://www.fedramp.gov/, 2015.

[7] The MITRE Corporation. FFRDCs – A Primer. http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf, 2015.