FEDERAL CLOUD & DATA CENTER SUMMIT

AUGUST 3, 2017 | MARRIOTT METRO CENTER | WASHINGTON, DC

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Cloud Collaboration Symposium held on August 3, 2017 in Washington, D.C. in conjunction with the ATARC Federal Cloud & Data Center Summit.

I would like to take this opportunity to recognize the following session leads for their contributions:

MITRE Chair: Justin Brunelle

Challenge Area 1: Innovation Challenges in the Cloud & Data Center Environment
Government Lead: Jason Boyd, HHS
Industry Lead: Greg Mundell, ScienceLogic
Industry Lead: Pete Nuwayser, Deloitte
MITRE Lead: Greg Barmine

Challenge Area 2: After the Migration: Pairing DevOps with Cloud Services
Government Lead: Peter Burkholder, GSA
Industry Lead: Scott Rutler, General Dynamics
MITRE Lead: Sunny Anand

Challenge Area 3: The Impact of Standards on Government Cloud Usage
Industry Lead: Hayri Tarhan, Oracle
MITRE Lead: Mari Spina

Challenge Area 4: Measuring the True Cost of Cloud
Government Lead: Mike Cassidy, DOJ
Industry Lead: Brian Bonacci, Infinera
MITRE Lead: Katy Warren

Challenge Area 5: Cloud Computing in Healthcare
Government Lead: Bill Cerniuk, VA
Government Lead: Dr. Joseph Ronzio, VA
DoD/VA IPO Lead: Chris Hills
Industry Lead: Mark Newsome, IBM
MITRE Lead: Audrey Winston

Below is a list of government, academic and industry members who participated in these dialogue sessions:

Challenge Area 1: Innovation Challenges in the Cloud & Data Center Environment

Robert Albert, NIH; Durga Anakala, HUD; Erneiliza Brown, USN; Casey Creech, MITRE; Rory Goosen, Deloitte; Christine Kim, MITRE; Ralph Kompare, Carbonite; Gopala Kuchibhotla, HUD; Manish Paliwal, USPS; Daniel Robinson, DOE; Robert Rourke, USA; Sahar Sadeghian, MITRE; Ty Schieber, GSA; Aisha Toussaint, Deloitte; Dan Twomey, GSA; John Tyler, IBM; Julie White, DoD-VA IPO; Bill Wright, 1901 Group

Challenge Area 2: After the Migration: Pairing DevOps with Cloud Services

Baha Akpinar, LOC; Kirk Brown, GDIT; Cisco DelCarmen, MITRE; Gian Dilawari, Dilnet; Jennifer East, FEMA; Guy Francois, DoD-VA IPO; Matt Friedman, MITRE; Joaquin Harley, GDIT; Karina Homme, Microsoft; Roopangi Kadakia, VA; Scott Kaplan, NGA; Imanuel Portalatin, MITRE; Retha Porterfield, IRS; Mike Tock, GDIT; Yolanda Washington, HUD; Kevin Wheatley, DOJ

Challenge Area 3: The Impact of Standards on Government Cloud Usage

Erneiliza Brown, USN; Adam Cowdery, DOS; Kevin Donohue, Leidos; Greg Griswold, US Department of the Treasury; Richard Hays, ANG; Aaron Kemmer, MITRE; Heideh Shadmand, DoD-VA IPO; Duron Shearn, DHS; Ann Williams, DOS; Pamela Wise-Martinez, PBGC

Challenge Area 4: Measuring the True Cost of Cloud

Marchelle Adams, US Courts; Nathan Bergman, DOJ; Ed Boriso, GSA; Mimi Boussouf, DoD-VA IPO; Aaron Cavanagh, FBI; Supriya Ganguly, Infinera; Neeraj Gupta, CFPB; Martin Isaksen, Cisco; Esmer Kanya, US Courts; Tina Meek, Microsoft; Adam Mendelson, Infinera; Ceresh Perry, USA; Michael Pyne, USN; Leonette Taft, VA; Wray Varley, Infinera; Shawn Watson, GSA

Challenge Area 5: Cloud Computing in Healthcare

Bart Bartholomew, DHA; Russell Davis, DHA; John Griffith, MITRE; Roch Kallymyer, McAfee; Cathlynn Metcalf, DoD-VA IPO; Mike Ross, DoD-VA IPO; West Coile, GAO

Thank you to everyone who contributed to the MITRE-ATARC Cloud Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)
Host organization of the ATARC Federal Cloud & Data Center Summit

FEDERAL SUMMITS

AUGUST 2017
FEDERAL CLOUD & DATA CENTER SUMMIT REPORT*

September 14, 2017

Justin F. Brunelle, Sunny Anand, Greg Barmine, Mari Spina,
Katy Warren, Audrey Winston
Mannan Javid, Aaron Kemmer, Christine Kim, Said Masoud
The MITRE Corporation

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

Contents

1 ABSTRACT

The most recent installment of the Federal Cloud & Data Center Summit, held on August 3, 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 and data center modernization. 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 and data center management techniques and best practices within the government.

Participants representing government, industry, and academia addressed five challenge areas in the federal cloud and data center domains: Innovation Challenges in Cloud & Data Center Environments; After the migration: Pairing DevOps with Cloud Services; The impact of standards on government cloud use; Measuring the true cost of cloud; and Healthcare IT.

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:

> Despite cultural resistance, proper DevOps practices are essential to effective government cloud adoption. Government cloud advocates should work to refine their DevOps policies and practices.
>
> Government cloud practitioners should drive the development and adoption of cloud security standards to help facilitate adoption among resistant cloud adopters.
>
> Other emerging technologies (e.g., Internet of Things (IoT), Artificial Intelligence (AI)) will help drive cloud adoption, and the government should prepare to "leapfrog" the trends in government technology adoption to prepare for the integration of cloud and other emerging technologies.

2 INTRODUCTION

During the most recent Federal Cloud & Data Center Summit, held on August 3, 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 and data center modernization. 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 and data center technologies and research in the government. Participants ranged from the CTO, CIO, 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) [15]. 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 Federal Cloud & Data Center Summit. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in cloud computing and data center management, 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 and data center 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:

- Innovation Challenges in Cloud & Data Center Environments;
- After the migration: Pairing DevOps with Cloud Services;

- The impact of standards on government cloud use;
- Measuring the true cost of cloud;
- and Healthcare IT.

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

3.1 Innovation Challenges in Cloud & Data Center Environments

The *Innovation Challenges in Cloud & Data Center Environments* session discussed barriers to enhancing innovation in cloud and data centers, explored opportunities for data center enhancement, and discussed current approaches to using innovation for data center modernization. Commercial cloud environments as well as on-premise data centers are prevalent in the government despite cloud receiving more attention, recently. Both require innovation to be as effective as possible and to advance government computing effectiveness. However, barriers such as policy, rate of acquisition, and others can prevent innovation from occurring in cloud and data centers. This session explored those barriers, opportunities to overcome them, and established recommendation for improving the government's ability to advance the state of innovation in cloud and data center environment.

This session had three goals:

- Describe challenges to introducing innovation;
- Recommend ways to overcome challenges; and
- Recommend best practices for data center modernization.

At the beginning of the session, the purpose of the session was reviewed, specifically mentioning that innovation challenges to be discussed included not only the cloud but the data center as well. Subsequently there were no discussions about the data center as the interests within the entire session focused on the cloud. The data center challenges could be summed up in one challenge, extending the data center into the cloud. This may be driven by the mandates in government to reduce the number of data centers and driven by the cloud first initiative; even when discussing – specifically – data centers, the conversation took a *cloud-first* direction.

Cloud security challenges have dominated many conversations and has received the lion's share of attention over the last several years. Although this challenge remains a concern, it did not make it into this group's "top 10" challenges in the order they were discussed. As

with many initiatives, agencies are hard pressed to identify where and how to begin cloud initiatives.

3.1.1 Challenges

The collaboration session discussions identified the following challenges prohibiting introducing innovation to cloud and data center efforts and environments within the government:

- Identifying the various expertise required to successfully migrate to the cloud
- Overcoming the cultural challenge for resistance to change (moving into the cloud)
- Attracting and hiring cloud knowledgeable resources in government
- Adopting disruptive technologies compounded by the rate of change
- Identifying migration priorities
- Understanding the acquisition processes for leveraging cloud services
- Adopting and integrating Software as a Service versus custom development
- Planning challenges, where to start and how to proceed
- Focusing on the return on investment versus costs
- Cloud Migration face the same challenges of Money, budgets and the color of money
- Security concerns with the use of open source software in the cloud
- Security and accreditation challenges
- Identifying changes to the operational model for sustainability within an integrated cloud environment

3.1.2 Discussion Summary

Despite a breadth of topics being covered by the participants in the session, a few were most actively discussed. These discussions are summarized – by topic – in this section.

The top challenge for innovation in cloud is the same challenge a lot of other IT initiatives face: finding the right talent; in this case with experience to effectuate a smooth transition to the cloud. This topic received the most attention as the government and their contractors

have a lot of experience managing data centers, much less for cloud initiatives. Participants felt that it was necessary to not only rely on contractor knowledge of the cloud but that in-house expertise was critical, as well.

Cloud experience is in high demand and industry throws generous incentives and salaries for those in the know. Training existing staff takes considerable time and energy and detracts from an already pressing workload.

The resistance to moving into the cloud remains ingrained in the culture within the government. For many seasoned veterans in the leadership ranks, embracing the cloud translates into taking on more risk without a clear understanding of the return on investment. With extensive data center experience, IT managers are asking themselves "why take on additional risk and expense of moving into the cloud? How is the value of using cloud resources measured? How do we go about justifying the cost, effort and risks associated with moving to the cloud? How do we switch the discussion away from costs to one focused on the value proposition?"

Cross generational technology from legacy systems to virtualized environments are difficult and expensive to integrate within an existing data center without the additional burden of moving them into and managing them in the cloud. The agency's mission and policy requirements often must justify the move of these systems into a cloud environment in order for them to be upgraded.

Acquisition for cloud services requires a different approach from traditional data center acquisitions and can present unique challenges, taxing the agency's resources which typically have limited experience in cloud acquisitions. Cloud technology continues to evolve rapidly adding another element of complexity to the acquisition process which can significantly impact the migration.

Moving into the cloud presents a major shift in paradigm for the Enterprise Services Lifecycle. The cloud offers many benefits to institute DevOps and accelerate delivery of mission capabilities. IT managers are again left with questions such as "How do we proceed, where do we start, how do we plan for this? How does this fit into the overall IT strategy?"

How does the cloud contribute to mission alignment? Migration into the cloud is not a lift and shift proposition; significant changes are required from a multi-dimensional perspective: human, cultural, moral, technology, policy and financial. Employees worry that moving to the cloud may render their skills obsolete.

The effort and the required resources to migrate could be considerable. The knowledge and experience required are instrumental. Reducing risk requires extensive analysis and can quickly bring a cloud initiative to its knees. How do government IT managers prepare an

entire organizational for this transformative shift and embrace this technological disruption?

There are different rules to play by in the DOD realm, one size doesn't fit all. Stringent security posture complicates all aspects of a transition to the cloud. The military may benefit the most from a cloud presence given the global distribution of the mission, yet has more challenges to overcome.

Post cloud implementation requires a different approach to sustainability; the challenges do not end with the migration. Understanding the operating model of the cloud is a new challenge which – in some aspects – may relinquish control of parts of the IT stack to different parties (except for a private cloud). The questions IT managers face include "How does supporting a cloud environment differ from the traditional data center? Managing resources in the cloud relinquishes control of those resources; where and how is government data physically stored as it may be distributed in multiple cloud locations; what are the challenges to importing or exporting vast amounts of data residing in the cloud?"

An open source architecture is more prevalent in the cloud than the traditional data center raising concerns about potential vulnerability threats such as "How potential threats are identified in a cloud environment. Who is responsible for identifying the threat, mitigating the risk and responding and coordinating disruptive events across multiple parties involved in the service chain?"

There are many SaaS[1] instances as well as tools for monitoring and automating management of a cloud environment. Determining what the services and tools offer, how to use them, what types of resources are needed to manage them, their suitability, is a daunting challenge requiring knowledgeable resources to discern the information.

Security remains a concern for moving into the cloud, but is not considered significantly more complex than for the traditional data center. Security has been a major concern for early cloud adapters, much has improved as in setting standards such as FedRAMP and vetting the ATO process.

3.1.3 Recommendations

The participants in the *Innovation Challenges in Cloud & Data Center Environments* collaboration session identified several important findings and recommendations.

Acquiring the correct talent for cloud initiatives can follow three tracks. Hire cloud experienced resources, contract with external cloud expertise and train internal staff. Contracting may be the quickest solution for acquiring the expertise, although all three recommendations

[1] The three service models of cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [11].

should be followed concurrently. Knowledgeable Presidential Management Fellows (PMFs)[2] and interns can be valuable resources, as well.

Follow up with an Analysis of Alternatives to identify fastest, lowest cost, least risk, optimal efficiency solutions. There may be several choices (e.g., SaaS, cloud migration, do nothing).

Plan carefully, include all resources that support the use of cloud early in the process, including the acquisition and operational resources. Learn from industry, as industry typically moves faster than the government. Have buy-in across the board including leadership and stakeholders. Create Integrated Project Teams (IPTs) to help integrate cloud projects. Define success criteria to effectively measure cloud initiatives, and manage and mitigate risks accordingly.

Bring in training and/or coaching resources to help with cultural changes to alleviate any obstacles to cloud migrations. Coaches can help foster successful strategies leading to a smoother migration. A good organizational change management will quickly assess where the barriers exists.

Start small, look for a simple migration, low hanging fruit to gain leadership and stakeholder buy in. Perform a pre- and post-mortem analysis to capture benefits and risks. Cloud can help effectuate a DevOps culture leading to better stakeholder involvement and satisfaction. Have a clear understanding of funding allocations, which color of money applies. Help leadership understand the return on investment versus the cost factor.

Evaluate the different technologies and capabilities. Vendors can help, although beware of false claims. Explore how the cloud provider meets requirements. Ask if the organization has the right tools to manage a cloud environment. Identify potential SaaS/PaaS instances to leverage. Determine if open source provides an acceptable alternative. Understand how cloud security is administered and how Authority to Operate (ATOs) are managed.

Develop a plan of what needs to change and how to effectuate change for operational support. The operational model will change as new participants (cloud brokers and cloud providers) are introduced into the support structure. Ensure there is a clear understanding of the service level agreements with them.

In summary, the nature of the recommendations followed a similar pattern of recommendations given for any disruptive technology; start with baby steps and proceed cautiously. Until the risks are clearly identified and the return on investment has been analyzed and understood, adoption will be slow, but much progress has been made in these areas.

As the government is risk adverse and policy constrained, rollout of cloud technology has been slow. Though there are many benefits for using the cloud; cloud technology requires

[2] `https://www.pmf.gov/become-a-pmf/overview.aspx`

a major shift in mindset "culture eats strategy for breakfast"[3], understanding changes to planning, acquisition, integration and operations activities. Cloud knowledge and experience which has been traditionally lacking in government is critical for any migration.

- Educate leadership and stakeholders on the risks and benefits of using the cloud. Communicate status and issues often with them.
- Start with low hanging fruit as in small simple projects to demonstrate quick wins and gain some experience and organizational buy in.
- Plan, plan and plan some more before proceeding with the rollout. Make sure the plan is well understood by those who will participate in the rollout to the cloud and with the stakeholders so that they understand what they can expect. Ensure that the correct resources have been identified and procured
- Provide adequate training and mentoring of cloud technology and operations in the cloud.

This approach is not unique to cloud adoption, it follows a pattern of experience and common sense. The cloud is becoming a ubiquitous IT resource, providing services to the government enabling them to focus on their core mission objectives. The cloud enables an agency to take advantage of DevOps bringing solutions to the mission quicker as well as universal mobility through a distributed computing environment as well as many other benefits.

3.2 After the migration: Pairing DevOps with Cloud Services

The *After the migration: Pairing DevOps with Cloud Services* session focused on the differences between standard management and operations for IT systems and their counterparts in cloud environments. Specifically, this session aimed to discuss organizational operations and dynamics that should change when migrating to cloud; explore and recommend Operations and Maintenance (O& M) and DevOps intersection points to optimize cloud usage; and explore cloud services that help enhance or enable these organizational changes.

While most organizations begin their cloud journey with a decision of whether or not to migrate and how to migrate, many organizations have not thought about how to effectively operate after the migration. In this session, participants discussed how organizational and

[3] A quote from the session.

operational dynamics should change to better suit cloud environments by leveraging DevOps for enhancing organizational outcomes.

This session had three goals:

- Recommended operational changes;
- Recommended O& M and DevOps cooperative changes or efforts; and
- Recommended cloud services that help enable these changes.

3.2.1 Challenges

The collaboration session discussions identified the following key challenges with migrating and adapting DevOps processes to best fit cloud and data center environments:

- DevOps Adoption Barriers;
- Organizational Transformation; and
- Driving Change.

3.2.2 Discussion Summary

The session began with capturing participants' expectations and the challenges that they encountered in adopting DevOps practices. Queries ranged from overcoming cultural barriers to implementing fully automated solutions that leveraged DevOps tools. Collation of those queries discerned common themes that warranted further discussion and collaboration. The following items were among the most actively discussed in this context:

- Leveraging DevOps for fiscally responsible Agencies;
- Cultural Aspects;
- Making Foundational Changes;
- Overcoming Organizational Barriers; and
- Policy Alignment.

Leveraging DevOps for Fiscally Responsible Agencies Commercial sectors move faster with DevOps because they have a hard monetary "bottom line" and are more willing to take risks, as opposed to government agencies which can be bound by citizens' services impact, public welfare driven urgencies, mission priorities, or other non-monetary considerations. Commercial businesses that are at risk of shutting down are more open to change than established businesses. However, owing to bearing of fiduciary responsibilities, budget cuts might help government agencies move to DevOps, because of the potential cost savings associated with DevOps paired with cloud adoption. Further, showing reduction in operational costs (compared to Total Cost of Ownership) might be a better motivator.

Cultural Aspects DevOps involves a mindset and an environmental change that is driven top-down and bottoms-up. Not only it is important to have management sponsorship stemming directly from its executive leadership, but all teams must buy-in to the culture to be successful. One should expect the need to get people to believe that DevOps/Cloud is "better" than what they are used to.

Making Foundational Changes There would be a strong need to determine the foundational changes required before implementing DevOps as a whole. There is a forcing function that led organizations to transition to the cloud. Despite shrinking budgets, expansive change has to be driven across the broader vendor, contractor, and government teams to maintain a positive mindset.

Overcoming Organizational Barriers DevOps potentially restructures organizations. Large silos must be broken before DevOps can work. It is strongly advocated to bring all teams to the table when discussing changes. One must be comfortable sharing information across organizations. Sharing is hard when information is power, hence the need to revisit changing of reporting and responsibility models.

Conway's law[4] (intended as a sociological observation) suggests that organization structure dictates its code structure. The law is based on the reasoning that in order for a software module to function, multiple authors must communicate frequently with each other. Therefore, the software interface structure of a system will reflect the social boundaries of the organization(s) that produced it, across which communication is more difficult.

Some organizations employ product-centric teams rather than competency driven teams for their business or product owners to help achieve organizational goals[5]. Silo'ed teams

[4] https://en.wikipedia.org/wiki/Conway's_law

[5] https://hbr.org/1978/07/strategy-is-different-in-service-businesses

may focus on the success of their team (often at the detriment of other teams) as opposed to product-focused teams which work towards a greater common goal. Best teams are cross-functional and enduring with single outcomes.

One of the easiest ways to re-organize in a matrix organization is to align similar services. One has to decouple outcome owner in contrast to decision owner[6].

Policy Alignment Many a times policies do not align to intended best practices, and that can cause delays and wasted resources. There may be a need to revisit policies to determine if the mandated policies may be revised or completely castoff. Compared to a more stringent "law" mandate, policies can be changed to accommodate what's at stake.

3.2.3 Recommendations

The participants in the *After the migration: Pairing DevOps with Cloud Services* collaboration session identified the following important findings and recommendations:

- Leverage Leadership Influence;
- Identify Holistic Performance Improvement Opportunities;
- People Development;
- Employ Non-Conventional Contracting Vehicles;
- Implementation Considerations;
- Technical Considerations;
- Unified Organizations; and
- Cultural Motivation.

Leverage Leadership Influence Have conversations with leadership to talk about business value of changes. The mindset and sponsorship of cloud adopter's *top-cover* will be essential to maintain momentum. DevOps can be very disruptive as it might place customers (i.e., citizens) at risk. Those challenges be overcome by introducing social concepts such as "first followers/early adopters" [12] – initially, a few people take calculated risks by trying and showcasing new methods until a critical mass is reached and the new concept becomes

[6] `https://hbr.org/1968/11/organizational-choice-product-vs-function`

adopted by mainstream[7]. Early adopters include people who are closest to the mission or need speed to delivery as with DoD and Department of Justice (DoJ).

More risk-averse organizations should look to move smaller/lower impact systems using DevOps to show impact, thereby focusing on the positivity of a potential outcome. These organizations should work with early adopters and select or address projects that show how DevOps works. Further, these organizations might have to go to executive levels to get management buy-ins for setting up a Project Management Office (PMO) for DevOps.

Identify Holistic Performance Improvement Opportunities One of the pieces of advice that surfaced was to create roadmaps using Value Change Mapping (i.e., walking through all activities from inception to delivery and determining activities that provide value and/or would need to be modified or eliminated). Avoid activities that lead to "Dark Scrum"[8] so that organizations could reap the benefits of the process.

People Development As DevOps practices mature, organizations can expect automated software development life-cycles processes that can help maintain compliance (such as security measures) without constant human intervention. Automation may make certain employees redundant, but people need to constantly evolve to account for change. The session participants recommended having mentors for people who are not familiar with DevOps and help them grow into new roles. There will be a relentless need to educate and train people on development, security, and maintenance operations (DevSecOps) or pertinent cloud skills. Additionally, security and application development teams may have to be part of the same team.

Government practitioners could anticipate learning in areas that would push people out of their comfort zones. A diverse skill set is key to success, so organizations should expose teams to situations to which they are not accustomed and build a culture of learning in operational processes. Lead by example by being "code savvy" – instill and encourage teaching and learning code development across all levels in organizational operations.

Employ Non-Conventional Contracting Vehicles Traditionally, procurement and accounting professionals expect flat-rate changes in cost. However, costs can fluctuate in the cloud. Hence, from a business perspective, getting the right contract is important.

[7] https://www.ted.com/talks/derek_sivers_how_to_start_a_movement
[8] http://ronjeffries.com/articles/016-09ff/defense/#fn:trans

Implementation Considerations From a resources perspective, getting the right skill-set is important. It is recommended that people working on implementation report directly to leadership to stress the importance of DevOps. Having DevOps associated directly with an agency's Enterprise Architecture Board would ensure that agile pursuits are based on sound technical ground.

Create coalitions – experience suggests that one should implement and maintain cohesion with various technical teams before moving to cloud. One should not wait until organizations move to cloud to implement DevOps.

Technical Considerations Shared service models may have to look for common platforms and toolsets across organization(s) to rationalize. One has to explore and define the set of common services that will bring value to the organization.

To sustain DevOps (post cloud migration), take a deeper look at all inter-dependencies. A possible approach might entail starting with the application layer and working one's way up. Creating common API's across agency might be a good step in that direction.

Early failures provide the opportunity for early recovery, as well. As a good risk averse practice, leverage cloud to make quick decisions. Best practices include building security in your processes such as conducting static code analysis right after code commits. With common services, it is possible to deploy the same security tools in traditional data centers as ones in the cloud. You might even explore the possibility of "DevOps as a Service".

Unified Organizations Achieving compliance with DevOps needs to span across vendors/platforms on a continuous basis. This includes Integrating Security practices with DevSecOps. A concerted effort that envisions a mindset of achieving "ATO in a day" might be the tipping point to lead change.

One must work together to build success for entire "duration" instead of a short "moment". Executive sponsorship, change management and communication are time tested principles that apply to DevOps, as well.

Cultural Motivation There was an uproar among session participants when this topic was suggested, invoking the response: "Shame people into doing the right thing!" Imbibe a culture with an asymptotic drive in having its people always doing the right thing. It was earnestly suggested that FFRDC representatives should develop whitepaper on DevOps culture.

3.3 The impact of standards on government cloud use

With increasing oversight, requirements, and standards for IT acquisition and management in the government, cloud computing – and its promise of cost reduction – is top on the minds of government IT professionals. In this session, participants discussed the impacts of government IT related policy and standards on commercial cloud adoption.

The session was structured to capture IT manager pain points and to foster an open discussion on associated issues and potential solutions. Specifically, participants were asked to address the following in sequence:

- Identify the government policies, standards, or requirements causing concern;
- Describe the impacts or issues associated with identified policies, standards, or requirements; and
- Provide suggestions for addressing issues or successful solution examples.

A vast majority of session contributors indicated a need for additional guidance beyond existing government standards. This is consistent with progressive growth in government cloud adoption. As agencies begin to execute their cloud adoption strategies or act upon their migration plans, management and worker tiers are forced to wrestle with new and emerging issues not previously addressed. This illustrates the tremendous value in collaborative cross-agency working groups chartered to address emerging issues and brainstorm solutions.

3.3.1 Challenges

The collaboration session discussions identified the following general challenge areas:

- Trusted Interconnection (TIC) Reference Architecture 2.0 [8] (Guidance Needed)
  Area of concern: Performance Impacts, Boundary Definitions, and Data Ownership
- Application Integration Standard (Guidance Needed)
  Area of concern: Architectural Design and Migration Architectures
- Data Standards (Guidance Needed)
  Area of concern: Schema, Transformation, and Handling
- Identity and Access Management (IDAM) Definitions (Guidance Needed)
  Area of concern: Group Policies, Directory Schema, Single Sign-on (SSO), and Multi-factor Authentication (MFA)

- Routing and Bandwidth Standards (Guidance Needed)
  Area of concern: Internet Access, Domain Name Server (DNS) Resolution, API Calls, and Quality of Service (QOS)/Service Level Agreement (SLA)

- Governance Standards (Guidance Needed)
  Area of concern: Boards, Processes, Decision Making

- Single Security Pane of Glass (Guidance Needed)
  Area of concern: Security Controls, API Exposed Data, FedRAMP [9] Requirements, Cloud Access Security Brokers (CASB) Solutions

- Continuous Integration (lack thereof)
  Area of concern: DevOps, Agile Programs, Change and Configuration Management (CCM)

3.3.2 Discussion Summary

Government IT managers continue to seek guidance with respect to cloud service access architecture. Participants indicated a desire to avoid the TIC for performance reasons and are hopeful for progress regarding the TIC Overlay and the TIC Ready Cloud. The need for architectural guidance in the handling of application migration and integration of cloud deployments with backend agency systems continues to be a paint point for government cloud adopters. Ultimately, government IT managers continue to seek reference architectures to guide cloud migration and implementation.

While reference architectures can be of significant value, sometimes simple policy is all it takes to break stalemate. Participants expressed uncertainty in cloud migrations activities surrounding the definition and secure handling of data moved to the cloud. Some expressed concern regarding data ownership once a data set was moved to the cloud. Some expressed concern over the right to audit data generated by a cloud customer's provisioned services. Others expressed concerns over who has the right to copy and reproduce data moved to the cloud. The participants cited standards as a way to alleviate (or at least guide the mitigation of) these perennial cloud challenges.

An interesting problem in Role-based Access Control (RBAC) emerged while discussing the need for IDAM standards. It is obvious that use of a cloud service provider's (CSP's) IDAM system could require a re-mapping of user roles, privileges, and groups when identity federation is not an option. Typical government agency RBAC structures have multiple legacy tiers and years of evolution. Accordingly, RBAC distribution trees can be very large and

granular. By contrast, the clean new environment of a fresh commercial cloud deployment may afford a reduced set of RBAC tree components or provide an opportunity for rethinking of the structure. Some participants expressed a desire for government standards regarding the definition of cloud user roles and privileges and their mapping to agency Global Policy Objects (GPOs) (e.g., Microsoft Active Directory™).

While migration and implementation guidance would typically seem sufficient for cloud adoption, lack of guidance regarding the execution of development, security, and maintenance operations (DevSecOps) is troublesome. Use of the commercial cloud has many implications for a broad spectrum of the organization. Each deployment can involve procurement, engineering, operations, security, and other departments. The automatability of cloud operations is forcing the move to agile management. Moreover, a large array of supporting cloud development and operations tools have emerged to create a state of paralysis by tool analysis as managers wrestle with tool selection. Finally, the availability of familiar operations and security data associated with commercial cloud deployments is causing operational entities such as cyber defense providers to think twice before committing to specific cyber SLAs.

The impact of commercial cloud adoption upon the totality of the organization is just now being felt by mid- and lower-level agency managers. As a result, the cry for guidance in governance rings loudly. Participants expressed a desire for agency specific guidance in governance regarding:

- Interacting with the FedRAMP Program Management Office (PMO) and internal procurement departments;
- Integrating commercial cloud solutions with modernization efforts and technical skills development;
- Evolving technical and operational policies to facilitate adoption; and
- Making migration go-/no-go decisions.

In short, government IT managers are calling for reference architectures for migration engineering and integration, DevSecOps guidance to guide operations activities, and governance models to facilitate interdepartmental and interagency collaboration and decision making.

3.3.3 Recommendations

The participants in the *The impact of standards on government cloud use* collaboration session identified the following important government IT Manager needed guidance to facilitate cloud adoption:

1. Orchestration Support;
2. Reference Architectures;
3. Data Policy;
4. IDAM Standards; and
5. Governance Models.

In the area of migration and operations, managers are stymied by the vast array of tool options and the unknowns associated with new cloud orchestration constructs. Although experience is likely to operate positively in this realm, until then, managers are looking for help integrating legacy data center with automated commercial cloud operations, new management interfaces, and CSP specific data logging, reporting, and alerting systems. More specifically, participants indicated a need for the Single Security Pane of Glass (SSPG) and FedRAMP requirements for common API data exposure to demystify cloud driven cybersecurity environments. While the notion of a CASB was offered as a solution, participants indicated success with a variety operations support tools including:

- MuleSoft[9]
- Talend[10]
- Jenkins[11]
- Red Hat Open Container Project (OCP)[12]
- HP Eucalyptus[13]
- IBM BlueMix[14]

[9] http://searchcloudcomputing.techtarget.com/definition/MuleSoft
[10] https://en.wikipedia.org/wiki/Talend_Open_Studio_for_Data_Integration
[11] https://devops.com/tag/jenkins/
[12] https://connect.redhat.com/blog/open-container-project-ocp
[13] https://www.wired.com/2014/09/hp-eucalyptus/
[14] https://www.ibm.com/cloud-computing/bluemix/what-is-bluemix

- Oracle Developer Cloud Service (ODCS)[15].

Deployment questions related to TIC connectivity, TIC Ready cloud availability, network topology, and connectivity to agency-based backend systems continue to hinder cloud adoption. Reference architectures addressing connectivity and routing topology with references to QOS/SLA characteristics is believed to have substantive value for design engineering departments.

Every agency has its own variation on information models and critical data needs. Each data set comes with its own sensitivity and associated risk management requirements. However, many agencies have not yet begun the task of categorizing or identifying the risk characteristics of their data. For example, in the Department of Defense (DoD), the Cloud Computing Security Requirements Guide (SRG) defines four "Impact Levels" [7] for data classification. Each Impact level (IL) has its unique data sensitivities and associated handling requirements. This helps immensely in the definition and selection of cloud services and associated security requirements. The Intelligence Community employs a "Data Conditioning" process to sanitize and tag data for migration to a cloud service environment (CSE) and to define handling and security requirements. However, only contract terms and conditions can address the ownership and handling rights issues. Government agencies are urged to support efforts to improve government acquisition regulations and to establish associated cloud service procurement guidelines to address such concerns.

While it is not envisioned that a single universal government RBAC policy tree would apply broadly across the government, it is reasonable to consider the value in developing agency specific cloud deployment definitions and associated legacy-to-cloud RBAC mappings. The biggest concern in this area is associated with a non-secure mapping of privileges that could result in some cloud user erroneously acquiring unintended right to access and manipulate data creating a security vulnerability. Though such would not necessarily be an intentionally created vulnerability, it is one that could result from simply poor due diligence.

Government has an opportunity to aid industry in helping to refine and standardize governance. Accordingly, government cloud adopters have a responsibility to strive to "get it right." If government managers are uncertain about means and protocols for interaction, processes and stakeholders for decision making, and organization structures for responsibility assignment and business executions, government managers are effectively unarmed on the commercial battlefield. Solution suggestions in this realm include review of the use of frameworks such as NIST Cybersecurity Workforce Framework [14] for personnel capabilities or the NIST Cybersecurity Framework for organizational functionality. Finally, the

[15] `https://cloud.oracle.com/developer_service`

concept of specific cloud computing governance constructs were recommended, including the following:

- Implementation of a Cloud Computing Governance Board (CCGB) to specifically address cloud migration initiatives and projects;
- Implementation of a Data Governance Process to ensure the readiness of data to be migrated and address risk factors; and
- Appointment of a Chief Data Officer (CDO) to exercise authority and control over agency data placed into the commercial cloud.

In summary, this session addressed many standards and policy issues associated with cloud migration and believed to be acting as an impediment to cloud adoption. The group being extremely knowledgeable in the plight of the government IT manager dealing with cloud strategy implementation, gave tremendously useful discussion of the issues and recommendations for future success. It is the conclusion of this group that the following actions will go a long way to smoothing the adoption and migration of government systems to the commercial cloud:

1. Use cloud orchestration tools;
2. Develop cloud deployment reference architectures;
3. Identify agency data sensitivities and define associated handling requirements;
4. Create standard cloud based RBAC structures and map them to legacy structures when federation is not achievable; and
5. Implement cloud specific governance models.

3.4 Measuring the true cost of cloud

Measuring the true cost of cloud session focused on the benefits of cloud computing that are often difficult to quantify. Participants explored the “soft impacts” of cloud adoption; discussed methods of measuring soft impacts as well as other costs; and discussed opportunities of using these measures to facilitate cloud acquisition. There are multiple ways to measure the cost and return on investment of adopting or migrating to a cloud environment. For example, common methods include migration costs or yearly operating costs. This session will explore the alternate measures such as the increase efficiency of operation or ability to

perform new tasking; specifically, this session will explore opportunities to quantify those impacts, and help new cloud adopters measure expectations when migrating and adopting the cloud.

This session had two goals:

- Itemize soft costs as well as metrics to measure them and
- Discuss the role of soft cost metrics in cloud acquisition.

The session was structured around the major component of cloud costs to foster an open discussion on identifying all the cost elements, discussing options for cost control, and potential optimizations. Cost components were grouped into major categories based on cost similarities and to address all costs in the available discussion time. Specifically, the categories were as follows:

1. Infrastructure,
2. Connectivity,
3. Security/Certifications/Mobile,
4. Access/Delivery/Mobile,
5. Operation/Automation,
6. Management/Policy,
7. Training,
8. Migration/Transition, and
9. People/Process.

3.4.1 Challenges

The collaboration session discussions identified the following challenge areas with quantifying the benefits of cloud adoption:

- Infrastructure and Platform,
- Systems and Applications,
- Connectivity,

- Security,
- Access/Delivery/Mobile, and
- Operation and Optimization.

These challenges are discussed in further depth in Section 3.4.2.

3.4.2 Discussion Summary

Each identified challenge was discussed at length in the collaboration session.

Infrastructure and Platform IaaS costs cover the usage of physical hardware including compute, storage, networking, native operating system, and hypervisors. It also includes the physical facility space and utilities (i.e. power and water). PaaS includes operating systems, middleware, and run time environments.

Infrastructure and Platform Discussion For IaaS and PaaS, many considerations impact total cost of cloud.

SLAs and QoS - many CSPs provide multiple level of SLAs akin to the "Bronze, Silver, Gold, Platinum" program. Each increase in the stand of SLAs increases the responsiveness and services to users, but at a relative cost increase. Government organizations migrating to cost can benefit from understanding the SLAs and which is the optimal combination of cost and service. An honest assessment of the performance requirements needed by the government can improve this process.

COOP - Disaster Recovery (DR) and Continuity of Operations (COOP) are potentially significant for the Federal government. Essentially, three types of backup and recovery exist to support DR/COOP: Hot/Cold (periodic backups to an environment that is not operation-ready), Hot/Warm (backups sent to network connected site with minimal capabilities), and Hot/Hot (complete copies of production software and data).

Systems and Applications SaaS includes both software and data, non-migrated applications and APIs, and potentially more elements depending on the SaaS. Cloud costs for applications and data include the cost of migrating to cloud, and the cost for operating within the cloud.

Systems and Applications Discussion For systems, applications and SaaS, many considerations impact total cost of cloud.

Readiness - To estimate the costs for applications, government agencies must analyze factors such as:

- Is the application cloud ready (does it have to be refactored, made more secure, etc.)?
- Is the data cloud ready, and where does it go (active storage, archival, redundant back up, geographically agnostic, secure encryption, etc.)?
- Number of application candidates; if there are a significant number of applications, some proportion of them will not be good candidates for migrating to cloud.
- Cost impacts for maintaining a hybrid environment can be quite high and need to be cpmsodered/
- 80:20 rule: 20% of apps might take 80% of the effort to migrate.

User Community - the larger and more complex the user community, the more a cloud migration and operation is likely to cost. A user community that is geographically dispersed, silo'ed, performs complex functions, or is growing with use of cloud technology will have higher demands and likely be running a more complex operation. Note that non-standard business processes that require high degrees of customization may also increase costs. Sometimes, migrating to a cloud solution increases standardization of business processes, which can increase automation and reduce costs per operation (or costs per user). However, if the user base also increases, the overall costs can increase due to this demand. The value proposition of this simultaneous increase might be beneficial overall, even if costs increase.

Functional Complexity - generally speaking, a very complex system is based on extremely large data sets, high compute needs, high network access demand, and at least some amount of specialized configuration or coding of special functions. Maintaining complex systems can also be costly in terms of development, testing, training, and other requirements. Security of complex systems is also usually higher than simple systems. Individually, each of these parameters can increase costs of cloud systems. Combined, these parameters sometimes act to increase costs significantly.

Architecture - the architecture of the cloud solution system can impact both the migrating costs and the operational costs of the system. Certain decisions, such as commercial cloud versus hybrid cloud, tiered data storage, and other considerations, may significantly impact cloud infrastructure costs. Data lifecycle costs may actually increase in some circumstances

due to the wide variety of options in the cloud previously unavailable. Increased network traffic, as users move out to the cloud may increase costs as the network communication lines are upgraded.

Security - Security constraints on architecture may require significantly increased network communications as queries and data responses are repeatedly validated through security mechanisms. Cloud access through Cloud Access Points (CAPs) in the DoD, or TICs in the non-DoD Federal Government, may place additional constraints on communications performance, necessitating redundancies, which increase costs.

Connectivity Connectivity refers to the Federal government's ability to connect to the internet and cloud services. It includes the following:

- In-house Network Infrastructure,
- Network Services,
- Remote Access,
- Resources and Expertise, and
- Content Delivery Network (CDN).

Cost Drivers that were identified as having a significant probability of impact for connectivity include the following:

- SLA and QoS,
- Architecture,
- Users,
- Locations,
- Spans,
- Security (TIC, CAP),
- Legacy,
- Locations of Data, and
- Capacity.

Connectivity Discussion At least one government representative reported spending a lot of time troubleshooting system issues because connection failure points existed in a cloud environment that previously did not exist with an on-premise data center approach. Connectivity issues included an unreliable or overwhelmed CAP/TIC, network latency lags, and vendors inexperienced with government security requirements that caused performance issues. Attempts to remedy these situations included redundant connection points, working with vendors to educate them and find solutions mutually, updating contracts, improving leadership familiarity with the entire network operations schema, improving the architecture, checking connectivity between multiple CSP's, and even checking time zones. One factor that clearly decreased issues and improved the cost and time to resolving issues was high quality staff, who were well informed of the situation, and were able to work as a team to identify and correct root causes of issues. Having network performance tools and a deep understanding of the network path from a monitoring location to the cloud is critical to understanding problems that arise.

Security Security refers to the confidentiality, integrity and availability for applications and data for correct processing. The collaboration session discussions identified the following security areas as appropriate security topics:

- Appliances/Applications and Tools,
- Expertise,
- Processes – Audit – Remediation,
- PCAP, and
- Reporting and Logs.

Cost Drivers that were identified as having a significant probability of impact for security include the following:

- FedRAMP,
- Best Practices,
- Technology Deployed,
- Risk Tolerance,
- Users,

- Key Management,
- API Security,
- Incident Handling and Forensics, and
- Mobile Device Access.

Security Discussion Due to the limited time available for discussion, the primary focus of discussion for security involved the tools. A primary cost consideration for any cloud acquisition is the requirements of the government security officer, agency mandates, and federal requirements that must be met. What are the policies and practices for data management, encryption, best practices, responsibilities, etc., and are the tools provided as part of the enterprise (i.e., provided already by the government), or are they the responsibility of the application/system owner, and therefore part of the cost?

There was at least one suggestion to ensure that security best practices were reviewed and understood by all stakeholders both *before* and *after* migration to cloud. The costs of changing security practices to include changes necessary to ensure cloud security are part of the migration costs. The cost of continuing monitoring and handling security in an operational cloud are part of cloud operations costs. For example, migrating to cloud may require a shift to user-based security models such as RBAC, or may require a robust identity management tool that can address user access from known points (e.g., in house) and unknown points (e.g., remote locations). The government must address the costs involved in maintaining security in a new, user-based environment. Many third party security solutions exist. Choice of the best security tools depends on the requirements of the security officer and the architecture of the total cloud technology environment. Regardless of the deployment model or service level, management of the encryption keys is a critical element of cloud security. The government should own and manage the keys.

Cost of security logs was raised as a concern. Depending on the CSP, commercial costs for large data files, including security logs, can be significant. Logs are often stored in active storage, and processed and routines for reviewing, then archiving, security logs can reduce these costs (archive storage is generally far less expensive than active storage). Location may also affect costs in other ways. Hybrid cloud security logging costs may be higher than other deployment models, for example.

FedRAMP certification can have a large impact on security costs for Accreditation and Authorization. Most government organizations typically do not have financial resources or time to sponsor a CSP for an agency Provisional ATO (PATO). Instead, look for FedRAMP

authorized solutions, or vendors who are in the process of obtaining PATOs for their services. Note that specific CSP services obtain PATOs, not the CSP as a whole. A self-assessment of the government agency's data sensitivity requirement can save the government in cost. The higher the designated sensitivity of the data, the higher the required number of controls, and the more costs are involved with the CSP. Requiring additional controls can also add to the time necessary to obtain the PATO.

At least one government representative recommended getting help going through accreditation process. While the process is getting easier, it is nevertheless a challenge. Expert advice can help avoid unexpected pitfalls. In addition, having staff with Commercial CSP certification can significantly improve the chance of successful ATO, and reduce the time and cost involved in achieving it. Further, if the agency security policy does not currently support cloud adoption, then resolve this issue before attempting a cloud migration. The costs involved in attempting a migration without security policy support can be prohibitive.

Risk management, including research and knowledge of cloud capabilities and security risks, is key to managing security costs. Federal agencies should conduct research in risks and be able to envision high-risk scenarios, and develop and apply risk mitigation practices. These scenarios might also include future user demands for mobile access, mobile phone APIs, and Internet of Things access to systems and applications; in short, a Bring Your Own Devices (BYOD) scenario. The security of these types of access points is a growing consideration.

Discussion ensued over whether security costs would increase or decrease over time. CSP's monitor, collect and provide extensive data that can be analyzed for cost optimization. This includes evaluating the security-related information to search for more cost effective processes, tools or security management capabilities. However, costs of incident handling, forensics, monitoring tools, security staff training, and general security training of a growing population of users may increase security costs and offset the potential savings.

Access/Delivery/Mobile While not currently a prevailing demand or capability across the Federal government, future user demands for mobile access, mobile phone APIs, and Internet of Things access to systems and applications; in short, a BYOD scenario is anticipated. The costs of providing access for these types of access points is a growing consideration.

Operation and Optimization Operation and Optimization refers to the use and continued improvement of cloud services, including cost control and optimization for value. The collaboration session discussions identified the following security areas as appropriate operation and optimization topics:

- Training,
- Automation,
- Governance,
- Analytics,
- Optimization,
- People and Process,
- Cloud Strategy,
- Cloud Billing,
- Migration, and
- Shadow Data Center.

Cost drivers that were identified as having a significant probability of impact for security include SLAs, but are recognized to be much more broad despite not being specifically discussed in the collaboration session.

Operation and Optimization Discussion Due to the limited time available for discussion, the primary focus of discussion for operations and optimization centered around training and cloud strategies.

Training - Training staff for cloud migration success is essential. Many types of training, and communication in general, can be employed, at different costs. Books, or online access to materials on cloud essentials, or specific reading, audio or video materials on tools or SaaS services may be available. It is generally considered that training staff is a cost effective measure to ensure that mission function continues in the event of technology change. Various options, such as bringing in vendors for group training (versus training each employee one-on-one), “brown bags” or “lunch and learn” sessions, use of tools such as Sharepoint, email, videos, etc. are all cost effective training tools.

Cloud Strategy - Migrating to cloud is essentially a mission and business decision. Having a strategy and business case can identify the cost factors and lead to a complete estimate of the total cloud costs. It can also work to identify and optimize the migration, therefore reducing risk and costs. In developing the strategy and business case, agencies may elect to reach out to partners and view their examples of lesson learned and reasons for success and

failures in cloud migrations and operations. Developing tactical approaches, including pilots and sandboxes, is very useful for experimenting with migration options in a cost effective manner. Using automation frameworks such as Puppet or Ansible can be very effective and save time and costs. Building repeatable processes and frameworks to enable the consistent assessment, planning and implementation of cloud migration projects, including costs and risks, can help leadership decision making, and support cloud adoption programs with minimal cost.

3.4.3 Recommendations

Measuring the total cost of cloud involves many factors, both technical and non-technical. Determining the specific costs is dependent upon the agency's readiness to move to cloud, the scale and complexity of the solution, and the current users' demand. Future considerations such as growth in demand, and integrating new devices will also have cost impacts. The following conclusions were reached regarding major cost factors in adopting cloud:

1. Security is usually number one
    (a) Sometimes most costly consideration due to many potential impacts
    (b) Factors include current policy, processes, compliance, update or replacement of security tools, and FedRAMP
2. Network & connectivity
    (a) Cloud may include requirements to increase network connectivity in house, increasing the cost investment to move to cloud
    (b) Geographically dispersed user base versus local organization impacts cost as outlined above
    (c) Security needs may have a significant impact on network costs
3. Migration Planning & Strategy
    (a) Building a business case helps increase awareness and understanding of specific factors to be addressed for a cloud migration program or project
    (b) Building a strategy defines the major steps, reduces risks, and controls costs
4. Compute & Storage

   (a) Compute costs may be optimized over time per unit, but demand increases may offset optimization savings

   (b) Storage costs may be optimized for active versus passive storage

5. Operation/Optimization

   (a) Mission expansion may increase costs over time

   (b) Standardization and optimization may reduce the cost per unit (i.e., cost per user) over time

6. Management Oversight (Culture)

   (a) Culture and management play a significant role in total cloud costs

   (b) Very difficult to measure

7. Train key people in order to maximize knowledge and control risk and cost

3.5 Healthcare IT

The *Healthcare IT* session focuses on aspects of cloud services and their uses in the healthcare domain. Government healthcare organizations are changing in how they administer and monitor healthcare. Patients' experiences outside of healthcare as well as new technology are enabling patients to take more ownership of their healthcare. This fundamental transformation of healthcare is challenging the government's underlying infrastructure, governance, analytics, and business practices.

This session's goals and activities are defined by the Veteran's Administration (VA) Inter Program Office (IPO) with MITRE guidance. This session had four goals:

- Explore the impact of the Internet of Medical Things (IOMT) in expanding the boundaries of healthcare, focusing on the following questions: What data should flow from the edge to inside, and what data (analysis) can stay on edge? What is the role of AI in these environments?;
- Analyze how healthcare is preparing an infrastructure that will provide "anytime, anywhere" digital health;
- Discuss incentives for patients to participate in cloud-based healthcare; and
- Identify recommendations for advancing cloud usage in the healthcare domain.

3.5.1 Challenges

The collaboration session discussions identified the following challenges unique to cloud adoption in the healthcare domain:

1. Strategic Approaches
2. Data Sharing and Ownership
   (a) Sensors and Devices
   (b) AI and Machine Learning (ML)
3. Standardization

3.5.2 Discussion Summary

The cloud can be both transformative and disruptive. The discussion items in this section were the most salient.

Strategic Approaches to using technology to solve problems and create new capabilities The government needs to consider strategic approaches and innovations that will solve problems and create new capabilities. The Federal Government should work to use technology to solve challenges in a healthcare system that comprises 20% of the Gross Domestic Product (GDP) since this figure is expected to balloon as the US population ages. The challenges include:

- Early detection to improve the wartime mission for the DoD;
- Government accelerated research and development (R& D) to make advancements in prosthetics;
- Telehealth; and
- Supporting the warfighter in austere environments with sensors, low bandwidth, AI, and metadata.

These challenges require a fundamental change in how we work with electronic health records (EHR). The government can lead research in this area. Ultimately, the healthcare community needs to determine how to put health into the hands of the patient, meaning that each person is responsible for his/her health records. It may be possible to “leapfrog over

current technology" and get to solutions more quickly. We cannot continue with incremental updates as these take too much time and are too costly.

The government has a role in leapfrogging as it would allow the healthcare system to move from a fee for service to fee for value and would allow providers to concentrate on population health (i.e., preventative medicine).

In the DoD, which currently allots 10% of DOD budget to healthcare, there are advances towards preventative health including:

- Congressionally Directed Medical Research Programs (CDMRP) [16];
- Advances in prosthetics; and
- Wearables for keeping patients healthy over time.

The VA gets the majority of the US Government healthcare budget. VA has a history of using public-private partnerships and 60% of its healthcare is from outside the VA system. On average a veteran spends 100 minutes per year at the VA.

Data Sharing and Ownership Emergency medical responders (EMR) often do not have the data needed to treat a patient. The healthcare community needs to provide the healthcare professionals with both the patients' historical data (greater than three years) and personal (non-clinical) data.

Data sharing falls across a spectrum from personal data to research data. Personal data is what the patient chooses to share:

- Sensors and analytics would drive the processes;
- Interactive systems would allow for data to be analyzed locally; and
- With more individuals using sensors, there would be more results to drive different answers and create big data.

We also need researchers to develop analytics using personal data to provide feedback to the patient. We need to break the cycle where healthcare researchers hoard data and do not share it with patients/subjects. Currently, the healthcare community lacks the time to research during medical events (life threatening or not). To generate the analytics to solve emergencies, the healthcare community must assure that:

[16] `http://cdmrp.army.mil/`

- Patients are asked to share data;
- Patients can download medical images to their mobile phones and Smart tablets; and
- Provide opportunities to leapfrog technologies.

Today, the healthcare community has nearly the required technology for devices and wearables but needs the analytics to complete the processes. Also, there are generational perception differences; millennials are more willing to share their data and are more connected.

The healthcare community should consider flipping the inside and the outside. The clinical data in the EHR is owned by the provider and the health data provided on the phone is owned by the patient. The role of AI is needed to analyze the sensor data to provide personalized analysis of the patient that includes confidence factors in a highly-regulated space. This would work something like the "check engine" light on cars. An alert would go to the patient to contact the doctor and could include suggested behavioral and lifestyle changes.

Outstanding questions for the government include: "How do we introduce these innovations into the VA system? What do we do post-event to put the patient in remission? What can be prevented?" For example, there could be applications in the app store for DoD and VA users to download tools that redirect the patient to a health solution. This is a paradigm shift that gives control of the health record to the patient.

In DoD, this could limit the average time in doctor's offices. With more data available, the patient and provider can discuss the clinical issues. If social data is also mined, this may reduce suicide rates. Use of genomics would supply family history data analogous to the check engine light. It would be like using the check engine light versus replacing the engine!

The incentive for providers is improved doctor ratings and having healthier patients.

Sensors and Devices Ideally, the healthcare community wants to place sensors in the home to channel the right data to the doctor without the patients having to come into the office. This is especially helpful for the VA cardiology patients and with DOD for warfighter sensors. It is imperative to sense the environment and not just the patient. Environment sensing can also help predict a pending incident, possibly prevent it, if not, then at least provide important information to responders and doctors. For example, suppose someone is diving and needs to be resuscitated; their dive computer contains temperature data about the environment, and temperature affects resuscitation. This data should all feed into medical intelligence system helping the patient to get healthy faster and for the DoD helping the fighter return to the force quicker.

In the VA, the Smart Home initiative[17] is an example of using sensors. Discussions regarding the sensors included the following topics:

- If a provider team is responsible for readmissions, they are more interested in home healthcare;
- Follow up after surgery requires the provider to spend time with the patient and time to document the visit, neither of which require payment for the provider's time; and
- The provider is paid when patient calls doctor.

Telehealth is another exciting advancement, refer to the Whitehouse site for the VA's interview[18]. Another example of telehealth is the X Prize for Medicine – better sensors with better data – better than in ICUs[19].

A key question remains: "how much data should devices send?" Some data is too big to transfer back and forth to edge devices, such as genomics data. Perhaps it is important to send error codes (connecting to the earlier discussion on inference on devices) – to save bandwidth – the ML model on the device only sends data when something unusual is detected. Error codes in healthcare are dangerous because they lack full definition.

While sensors can be great, the healthcare community would be remiss if it did not mention the worry about cyber security. For example, what happens if a hacker gets onto a personal device.

Artificial Intelligence and Machine Learning Sometimes a provider does not need extensive historical data. For example, a doctor in an emergency room does not need 20 years of data. However, to be predictive, preventative, and proactive, one needs to be able to build models that use personal history to detect anomalies. Scenarios need to include what happens before and after an incident. Left of incident – borrowed from military/counter-terrorism term "left of boom" (e.g., what to do before an IED explosion happens versus what to do right of boom or after it happens?).

- The healthcare community needs systems that take the data from current incidents and learns personalized patterns; this is computer intensive. Once ML models are trained, the models can be pushed to edge devices.

[17] https://www.va.gov/HEALTH/NewsFeatures/2016/May/A-Smart-Home-for-Veterans-with-Brain-Injuries.asp

[18] https://www.whitehouse.gov/the-press-office/2017/08/03/remarks-president-trump-department-veterans-affairs-telehealth-event

[19] http://tricorder.xprize.org/

- Inference scenarios (requiring less computer intensive) from models can be used (on small devices) to detect unusual or concerning patterns and ignore expected or insignificant patterns. This can be used on the device to alert users/patients to issues.
- AI devices need to build that can alert the user and the doctor to healthcare issues; imagine having a heart attack and the smart watch makes the alert.
- Systems need to be mixed-initiative: Sometimes the system notifies the patient of a situation, other times, the patient needs to be able to ask the system for information, for instance if they are feeling "strange", or to ask follow-up questions on system alerts.
- Some argue that the healthcare community does not need to worry about language processing and should just concentrate on amassing data from health devices or in databases. Human observation cannot at this point be replaced by just lots of data. Doctors' comments and patients' conversations contain important context that cannot be detected by health devices and ML. ML is powerful, but it is not magic.

Regarding the role of augmented intelligence, the healthcare community needs to process on the edge and determine the bandwidth. Tools and platforms currently exist today to boost cognitive / augmented intelligence capabilities to help prevent suicides by the following:

- Building emotional resiliency in those at risk for suicide far in advance of ideations by leveraging augmented intelligence and chatbot technology and
- Analyzing social media and other data sources to understand the sentiment, tone and emotion, allowing us to quickly assess whether an individual is of suicidal risk not.

These tools can be leveraged to both pre-screen Veterans for early signs of suicidal thoughts, and to foster emotional resilience via a trust platform that seeks to first understand the individual and then reason from inputs, needs, and services. Available tools teach individuals to provide an interactive chatbot environment whereby the data is user-owned, available on mobile devices, and leverages available services or user-selected peer networks to build resilience far ahead of suicide contemplation.

Be aware that AI works using confidence factors. System confidence is not sufficient. There are plenty of examples where systems report 99% confidence and are completely wrong in ways that are obvious to a human.

Standardization New EHR addresses interoperability issues, but it will not fix them. The healthcare community needs standard workflows to save money on fixing data and to organize nonstandard data. The healthcare community must also realize that humans will still make mistakes.

VA systems have the reputation of not being interoperable; however, they have more than 90% standardization yet we have less than 1% of medical data in EMR systems. Currently, providers need only need three years of old data, but we will need more data for predictive analysis.

EHR provides standardization between Departments and currently it is only used for medical documentation. Open API standards have an impact on healthcare, but to do so, they must do the following:

- Make sense;
- Allow users to establish a relationship;
- Allow for agreement on data storage; and
- Allow for the extremes – personal information versus research.

Current discussion about healthcare standards can be found at IEEE 11073 (Health informatics - Medical / health device communication standards)[20].

3.5.3 Recommendations

The participants in the *Healthcare IT* collaboration session identified the following important findings and recommendations:

- The government needs to consider strategic approaches and innovations to help solve problems and "leapfrog over the current technology" to create new capabilities;
- The healthcare community need to move towards a mindset where patients own their data and choose to share it with the providers through wearable devices and sensors. This provides two significant advances:
  - Researchers can use the data and scenarios to build AI systems that will be predictive in nature and

[20] `https://en.wikipedia.org/wiki/ISO/IEEE_11073`, `https://standards.ieee.org/findstds/standard/healthcare_it.html`

  - When patients are sick or injured, the environmental and personal data is known, allowing patients to be treated quickly and efficiently, reducing further complications, and getting him/her healthy more quickly.

- The healthcare community must have standardized workflows to build the infrastructure needed to transform health systems; and
- Preventative health is the ultimate goal.

4 SUMMIT RECOMMENDATIONS

As with past Federal Cloud & Data Center Summit discussions, the collaboration sessions discussions had a common set of themes.

As cloud adoption becomes more prevalent within the government, the shortage of appropriately trained individuals is becoming more apparent. To help alleviate this challenge and while government representatives are becoming trained, **public-private partnerships can help alleviate the skillset shortage of cloud practitioners in the government**.

Government IT managers have called for **reference architectures, migration guidance, and governance standards to help guide cloud adoption and decision making**. These standards will help organizations migrating or adopting clouds for the first time navigate the process of using cloud services.

DevOps will become of utmost importance, and guidance documents on how to adopt DevOps will be essential to ease the transition to cloud environments that modify current government agency practices.

Security – a perennial challenge of cloud adoption – would benefit from **a SSPG or common CSP security-related API standards** to simplify the integration of cloud-based cyber defense solutions for agencies working across multiple cloud platforms.

5 CONCLUSIONS

The August 2017 Federal Cloud & Data Center Summit highlighted several challenges facing the Federal Government's adoption of cloud computing and data center modernization efforts.

- The primary barrier to government cloud adoption remains cultural aversion (e.g., "letting go of the data", adopting proper DevOps)

- Accurately measuring and predicting cost is challenging, particularly the impacts of cultural changes on overall cost
- Standards – particularly those addressing security – are vague and have not yet helped broaden cloud adoption in the government
- "Leap-frogging" (i.e., planning and preparing for the latest and next technical evolutions) technology is essential to helping government keep pace with industry

The focus of the discussions is shifting toward "IT managers" (e.g., policy and intra-agency adoption) as cloud implementations become more accepted, trusted, and common-place. However, cultural barriers still exist, making government cloud adoption (as well as its cost estimation and preparation) more challenging. Specific to cost estimation, tools exist to make cloud operation costs well understood and estimated, but managerial and cultural costs are still difficult to properly and accurately estimate.

As cited, the government is traditionally "good" at using, implementing, and operating in data centers, but the translation of those skills to cloud environments has been difficult. Despite those challenges, government representatives understand and have adopting the mindset of "cloud-first".

The emphasis of DevOps and how good DevOps practices can help facilitate the migration to and adoption of cloud services occurred in nearly every collaboration session. This reinforces the need for government agencies to revise their DevOps practices when considering a migration to the cloud.

While the August 2017 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. Contrary to prior summits [4, 5, 6, 3, 2], there were a variety of "cloud champions" advocating for the rapid adoption of cloud services, cloud-first adoption, and risk-taking for cloud adoption. Further, the security challenges traditionally mentioned along with cloud adoption have moved from universal aversion to more granular issues. For example, the participants cited the need for enabling standards, monitoring controls, and interoperable APIs for better monitoring of cloud-based data.

An interested theme from the day was the notion of needing a *forcing function* that will help expedite proper cloud and DevOps adoption within the government. Many participants cited budget cuts as a looming forcing function of cloud adoption; in other words, cloud adoption would help push cloud adoption and streamline the process of enhancing technological innovation and modernization. The forcing function may also be the increased

value of integrating multiple emerging technologies into a cloud environment, such as IoT or mobile [10].

In a change from prior years [13], the summits will be held less frequently[21], opting instead for an increased emphasis on working groups. ATARC is holding a series of working groups – to include a variety on the topic of cloud computing [1] – to address the more granular challenges and nuanced needs of government cloud practitioners. This follows the summits' own recommendations for emphasizing collaborative working groups. We recommend that government cloud practitioners participate in the appropriate working groups to leverage best practices, influence policy and practices, and facilitate government cloud adoption. Per the recommendations of this document, participation in these groups is highly recommended for government cloud practitioners and organizations that support government cloud adoption.

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[22].

REFERENCES

[1] ATARC. Atarc cloud innovation lab. `https://www.atarc.org/working-groups/cloud/`, 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 & data center summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[21] Please see `https://www.fedsummits.com/` for the schedule of upcoming summits.
[22] `http://www.fedsummits.com/cloud/`

[3] J. F. Brunelle, D. Davis, D. Huynh, M. Malayanur, B. Natale, H. Small, T. Harvey, and T. Suder. January 2016 atarc federal cloud computing summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[4] K. Caraway, D. Faatz, N. Ross, J. F. Brunelle, and T. Suder. July 2014 federal cloud computing summit summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2014.

[5] K. Caraway, N. Gong, M. Kristan, N. Ross, J. F. Brunelle, and T. Suder. January 2015 federal cloud computing summit summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2015.

[6] K. Caraway, N. Gong, J. Packer, J. Vann, J. F. Brunelle, T. Harvey, and T. Suder. July 2015 atarc federal cloud computing summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2015.

[7] Defense Information Systems Agency. Department of defense cloud computing security requirements guide. Technical Report Version 1 Release 3, Developed by the Defense Information Systems Agency for the Department of Defense, 2017.

[8] Federal Network Resilience. Trusted Internet Connections (TIC) Reference Architecture Document Version 2.0. Technical report, Department of Homeland Security, 2013.

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

[10] T. Harvey, T. Suder, M. Peck, G. Seth, M. Russell, P. Benito, and M. Collins. August 2015 federal mobile computing summit collaboration session summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[11] P. Mell and T. Grance. The nist definition of cloud computing: Recommendations of the national institute of standards and technology. Technical Report Special Publication 800-145, National Institute of Standards and Technology, 2011.

[12] G. A. Moore. *Crossing the Chasm.* Harper Business, 2014.

[13] G. Mundell, K. Jones, and V. Subbiah. Cloud & data center working group. `http://www.atarc.org/innovation-labs/cloud/`, 2016.

[14] W. Newhouse, S. Keith, B. Scribner, and G. Witte. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Technical Report NIST Special Publication 800-181, National Institute for Standards and Technology, 2013.

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