FEDERAL SUMMITS

JULY 2015
ATARC FEDERAL CLOUD COMPUTING SUMMIT REPORT*

October 20, 2015

Karen Caraway, Nicole Gong, Julia Packer, Jim Vann, Justin F. Brunelle
The MITRE Corporation†

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

†The authors' affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the authors.

Contents

1 EXECUTIVE SUMMARY

The most recent installment of the ATARC Federal Cloud Computing Summit, held on July 23rd, 2015, included four 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 four challenge areas in federal cloud computing: DevOps and Automation in the Cloud, Integration Services and Migration Aids, Acquisition and Contracting for Cloud Services, and Data Interchange in Federated Clouds.

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

- The perennial challenges (e.g., security, adopting agile processes, cultural issues with acquisition) that have existed in the cloud domains are still perennial challenges. However, the challenges are no longer at the level of Cloud in general but instead are at lower, finer grained levels of the process (e.g., the cultural challenges facing acquisition are at the level of DevOps adoption within the cloud rather than cloud adoption, itself).

- Challenges with education still exist, but rather than receiving education on general cloud concepts, practitioners should be educated on how existing processes within the government can be adapted to better support cloud.

- Advances are being made with respect to cloud acquisition, but more work is left to be done. Cloud Service Providers (CSPs) are beginning to adapt processes to facilitate government cloud adoption, and the utilization of 3rd-party or open-source utilities can aid in migration.

2 INTRODUCTION

During the most recent ATARC Federal Cloud Computing Summit, held on July 23rd, 2015, four 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.

The MITRE Corporation [8] is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs). ATARC is a non-profit organization that leverages academia to bridge between Government and Corporate participation in technology. MITRE worked in partnership with ATARC to host these collaborative sessions as part of the ATARC Federal Cloud Computing 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 academic while identifying cross-cutting issues between the challenge areas.

3 COLLABORATION SESSION OVERVIEW

Each of the four 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:

- DevOps and Automation in the Cloud
- Integration Services and Migration Aids
- Acquisition and Contracting for Cloud Services
- Data Interchange in Federated Clouds

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

3.1 DevOps and Automation in the Cloud

The DevOps and Automation in the Cloud session discussed best practices for end-to-end management for cloud services along with tools that can facilitate and enable cloud service management and optimization. The goal of the joint session was to outline recommendations for best practices and tools, services, and utilities for cloud management automation; identify challenges with cloud service automation; assist non-technical cloud practitioners with cloud management; recommendations for integrating IT operations and orchestration with DevOps; and highlight the differences between cloud and non-cloud systems DevOps within the government.

The goals of this session included discussions of the following:

- End-to-end cloud system management
- Best practices for cloud DevOps
- Tools for cloud DevOps and service automation
- Traditional government DevOps practices and applicability for cloud systems

3.1.1 Challenges

The collaboration session discussions identified the following DevOps and automation challenge areas or needs:

- Define a process for identifying quick wins, and define metrics for recognizing success.
- Educate decision makers and practitioners regarding the challenges at various levels of DevOps, as well as define DevOps for the cloud.
- Create site accreditation and templates for operating in the cloud.

3.1.2 Discussion Summary

The DevOps and Automation in the Cloud session identified several challenges regarding the adoption of traditional DevOps processes in a cloud environment that is designed to be scalable; similar to the perennial challenge of migrating legacy systems to the cloud within the government, adapting DevOps can involve cultural, educational, and operations based

challenges. Automation is often associated with DevOps, with the goal of facilitating service management.

DevOps within the cloud impacts changes in governance, staffing, and cultural perceptions of operations, security, and compliance. Automation impacts the security, governance, and policy of cloud adoption. The session participants cited that current cloud DevOps are top-down and rely on waterfall-style models. DevOps encompasses the entire life-cycle management process of an application in the cloud. As such, it is important for cloud practitioners to balance the benefits with the time, resources, and cost of implementing new processes within the cloud environment.

Because some DevOps processes are already implemented in the cloud as services from cloud service providers (CSPs) and as processes in place by peer government organizations, government practitioners should reach out to peers for success stories and best practices. In particular, crowd sourcing – even within the sub-environment of the government – can be useful. Jenkins [4], Chef [1], and other open-source tools can be valuable and help with code analyses.

3.1.3 Important Findings

The DevOps and Automation collaboration session participants identified the following recommendations:

- Identify quick wins, or easy adoption targets for refining DevOps processes.
- Identify tools to help DevOps, potentially from open-source utilities or third-party sources.
- Streamline legacy DevOps processes to be better suited for scalable services.

3.2 Integration Services and Migration Aids

The Integration Services and Migration Aids session discussed the challenges and best practices for migrating legacy applications to cloud platforms. The goal of the joint session was to outline recommendations for migration strategy best practices, including identifying features of cloud-ready applications, migrating from cloud-ready to cloud-enabled, and services for integrating cloud services (e.g., leveraging a heterogeneous CSP landscape, or adopting a hybrid cloud approach). This includes identifying a recommended migration process as well as identifying migration tools and services.

The goals of this session included discussions of the following:

- Recommend migration best practices for CSP, public, private, and hybrid cloud environments
- Identify services and tools to facilitate cloud migration
- Identify challenges for migrating to the cloud
- Identify features of cloud-ready applications

3.2.1 Challenges

During the collaboration session, the participants identified several challenges that should be addressed to advance the state of cloud computing in the federal government.

These discussions identified the following challenges:

- Establishing communications across multiple and different clouds and CSPs
- Identifying data and applications/services suitable for cloud migration
- Identifying and mitigating risks during and after migration
- Identifying suitable 3rd-party or open source tools for aiding in cloud migration
- Some legacy solutions may not be suitable to migrate to the cloud (cannot be virtualized, for example)
- Some legacy solutions would be better updated prior to migration (not just a "lift and shift")
- Some cloud providers can support both virtual servers and virtualized server environments, as well as physical servers (e.g. baremetal on SoftLayer [7])
- If a government agency moves software and data to the cloud, how will you achieve the performance needed for the end users and the connected systems not in cloud?

3.2.2 Discussion Summary

The Integration Services and Migration session started with a discussion of the Five Layers of Conceptual Architecture framework as a launching point for the discussions (Figure 1). The first layer identifies the mission spaces' needs for stakeholders, the second layer represents the needs for the Enterprise Information Technology (IT) Legacy environment, and the third layer

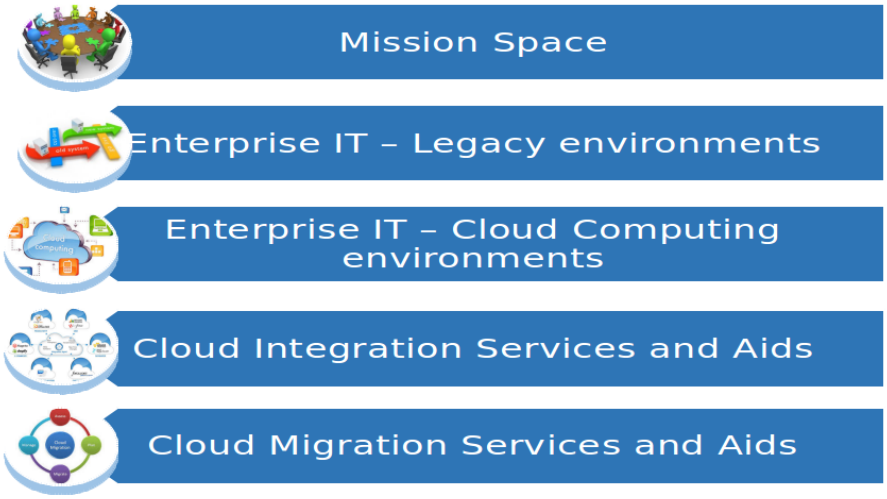

Figure 1: Five Layers of a Conceptual Architecture

represents the needs for the Enterprise IT – Cloud Computing environments. The working group agreed that cloud practitioners need to understanding the legacy environment along with the potential migration environments to effectively migrate legacy services to cloud environments. Layers four and five identify the needs and requirements for the integration service and migration services.

The Cloud Migration Life-Cycle starts with the assessment process, which includes assessing the legacy systems and workloads to be migrated for cloud readiness. This assessment allows organizations to determine what migration candidates (systems and data) can and cannot migrate to a cloud environment and what type cloud (e.g., public, private, or hybrid) will be a suitable migration target based on the features of the legacy system. Organizations should develop decision criteria for the suitability and readiness assessment processes. The session participants recommend that agencies beginning their first cloud migration start with lower risk systems which contain minimal customer and sensitive data and take advantage of the cloud's elasticity to grow from this point forward. Alternatively, agencies should identify which systems are not suitable for cloud migration.

The working group suggested several readiness assessment areas to include several aspects of the assessment process:

- Business Considerations – Evaluate the overall organization readiness, important of the systems to the business or the mission, the risk tolerance level of the business, and organization culture (i.e., favorable or resistant to change).

- Systems Life-Cycle Considerations – Identify the life-cycle stage of the migration pro-

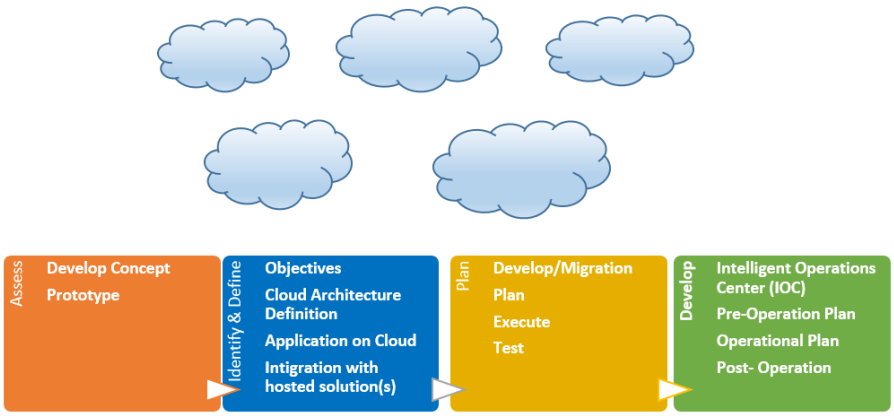

Figure 2: High-level Life-cycle for cloud migration

cess (e.g., in complete redesign or in a technology refresh). This helps identify and measure the benefits achieved from migrating to a cloud environment.

- Data Constitution – Identify the data governance, confidentiality, integrity, and quality that must be preserved during the migration to define the rigor and fidelity required of the migration process.
- Security Consideration – Target environments for cloud migration are of particular importance. For example, the application owners should identify whether or not CSPs are responsible for security controls, identification and correction of system vulnerabilities, and defense against specific cloud-oriented attacks. Requirements for these protections should be put into service level agreements.
- Technology Consideration – Similar to security, the migration environment should be assessed for performance, storage, and other technical requirements.
- Integration Consideration – Systems dependencies, data integration (e.g., sharing storage or file systems), or presentation integration concerns should be considered before selecting a migration target.

The cloud migration life-cycle continues with the development of a proof of concept prototype, identification of objectives, architecture definitions, planning the development of the Intelligent Operations Center (IOC) (which includes pre-operational requirements, operational requirements, post-operational requirements), and concludes with the End of the Life-Cycle. Figure 2 presents the high level life-cycle the session participants created.

Accompanying the high level life-cycle diagram, the session participants identified a process for cloud migrations.

1. Objectives Definition – Including Key Performance Parameters (KPPs)
2. Request For Proposal (RFP)
3. Proposals Review and Neck Down
4. Competitive Selection to Contract Award
5. Program Start
   (a) Iterative, Incremental DevOps Cycle
      i. Planning
      ii. Development
      iii. Test
      iv. Deployment to Mission Operations environment
   (b) Assess and Repeat (i to iv)
6. Program End
7. Assessment and Lessons Learned

The collaboration session ended by identifying a set of topics that still need to be discussed and questions that remain unanswered that should be addressed at future collaboration sessions:

- Migration
  - What are the barriers preventing the smooth migration?
  - What is the budget and schedule for the migration? Is risk tolerance a factor?
  - What is the mission area and considerations for the migration?
  - What do government executives need to know in order to develop a cost effective cloud migration plan?
  - What are the logical progressions or roadmaps to ensure all stakeholders are involved in migration strategy?
  - How should the government progress through the layers from defining mission objectives to migration plan?
  - Are there tools to help assess the migration suitability and readiness analysis?

- What are the standards for migration?
- How should the government treat legacy applications that cannot be migration?
- How can a cloud migration checklist be converted into a migration rating system?
- What issues impact cloud portability and standardization?
- What issues impact cloud interoperability and security capabilities?
- What are the success factors for integration?
- When selecting the cloud service, is it difficult to have the PaaS with one provider and the SaaS or IaaS with another provider?
- How will cloud providers comply with two factor authentication?
- What integration challenges exist between legacy and modernization systems
- What are the requirements for private cloud solutions for government?
- How should the government tackle the public cloud and private cloud integration issues?
- Are there methodologies, commercial tools, or services available to support cloud DevOps?

3.2.3 Important Findings

- Recommended a high level architecture and process for cloud migration
- Identified current, top challenges for legacy to cloud system migration

3.3 Acquisition and Contracting for Cloud Services

The Acquisition and Contracting for Cloud Services session discussed the current challenges – as well as recommendations for overcoming the challenges – with contracting approaches and processes for procuring cloud services in the government. The goal of the joint session was to outline recommendations for identifying and overcoming cost challenges, identifying contracting vehicles for cloud services, discussing challenges with Federal IT compliance during cloud acquisition, and discussing the differences between federal and commercial cloud service providers.

The goals of this session included discussions of the following:

- Identify best practices, contracting approaches, and vehicles for cloud services

- Identify challenges with federal IT compliance and perceived incompatibilities with cloud acquisition
- Recommend purchase agreements for variable cloud use
- Identify costing concerns for cloud migration

3.3.1 Challenges

These discussions identified the following challenges in the areas of cost, designing pay-per-use agreements, getting better cooperation from cloud providers, choosing contract types, and ensuring compliance with government requirements.

3.3.2 Discussion Summary

Participants in the Acquisition and Contracting for Cloud Services session discussed the current challenges associated with contracting for cloud services within the government – as well as recommendations for overcoming these challenges. Session participants engaged in discussions in the following areas:

- Agency Cost Concerns
- Designing Pay-Per-Use Agreements
- Are Cloud Service Providers helping?
- Which Contract Vehicles & Types Are Best?
- What are Biggest Compliance Challenges?
- What Other Issues are emerging (e.g., is workforce training sufficient?)?

The collaboration session discussions focused on several topics including agency cost concerns, designing good “pay-per-use” agreements, identifying how CSPs have helped government cloud contracting, understanding which contracting vehicles are best for cloud, compliance challenges, and other areas of importance.

3.3.2.1 Cost Concerns With the emergence of the White House Cloud First Policy [5], cost savings were widely assumed to be the major reason for moving to cloud solutions. However, session participants noted a recent shift among industry and government leaders, suggesting that the less tangible benefits of efficiencies and productivity may provide a better justification for moving to cloud solutions than potential cost savings. Early cloud computing initiatives captured "low-hanging fruit," such as cloud-based e-mail and Infrastructure as a Service (IaaS) projects with modest investment requirements and risk. Now, as cloud moves to supplant legacy systems for more complex deployments involving core mission needs and higher security requirements, cost savings must be clearly established via rigorous business cases. Better cost estimating techniques, including Return on Investment (RoI) analyses of alternatives and business case methodologies will be essential.

Simply not having enough money in the IT budget continues to be a key concern of agencies. Budgets are under ever increasing fiscal pressures and uncertainty – especially given the critical needs for information assurance and cybersecurity. With tight budgets, there is little desire to experiment with new commodity cloud products unless and until they meet core mission needs and their business cases reveal significant RoI benefits. Contracting Officers (COs) can be expected to demand solid business cases, Analyses of Alternatives (AoAs), and Independent Government Cost Estimates (IGCEs) to justify any proposed cloud alternatives. Panelists and participants in the session agreed that more quantifiable and rigorous pricing analyses is needed to support the case for buying cloud in the face of competing demands for IT expenditures. This will have broad implications for budgeting and acquisition practices across the Federal government.

While early Federal mandates created high expectations to "move faster to the cloud," Session participants reported that their agencies are making steady progress toward cloud solutions. However, It is difficult to rationalize major new cloud initiatives when mission critical legacy systems and security mandates are competing for the same budget resources. One question was posed to the participants: "How many of you have submitted your Fiscal Year cloud budget information?" None of the Session participants responded in the affirmative, possibly indicating how little is being done to communicate budget priorities and guidance for cloud spending. Participants discussed the new Office of Management and Budget (OMB) requirements for agencies to capture and report cloud spending by IaaS, PaaS, and SaaS categories and deployment types. However, in order to take cloud acquisition to the next level, it may be necessary to issue more detailed guidance and enforceable policies than what was first established in "cloud first."

3.3.2.2 Pay-per-use Agreements Current Federal procurement practices favor firm-fixed price contracting in which delivery requirements are firmly established in advance. The use of Time and Material (T&M) and cost reimbursement type contracts, which may provide for more flexibility in situations where usage is uncertain, is increasingly discouraged within agencies. Further, current IT contracting practices have been designed around the delivery of hardware and labor services. Consumption-based cloud computing, by its nature, does not lend itself to these traditional procurement practices.

Participants noted that commercial cloud providers expect customers to know in advance exactly how much service will be required. Even if contractual vehicles were made more flexible, program element budgeting practices within agencies make it difficult to reprogram funds when actual usage varies from what was budgeted. Session participants agreed that this issue is very complicated, since it involves both financial and acquisition management policy areas. While paying "only by the drink" may sound like an attractive business model, it requires new disciplines and an overall culture change on the part of the user. In the DevOps environment, it is easy to unknowingly run-up usage charges that are discovered only when it is too late. One participant likened the problem to checking out of your hotel and suddenly realizing that you were billed for the shampoo or electricity used. "Getting people to turn out the lights when they leave the room is a management issue – not always easy."

While the terms and conditions of billing may be established in the contractual fine print, they are not always understood at the user level. Some providers prefer to invoice by "customer accounts" which may have little meaning to users and complicate the estimate of usage within a billing cycle. As a result, the provider often has the upper hand when costs are charged. The need for new mechanisms for usage governance was discussed. "Not-to-exceed" and "limitation-of-costs" clauses have been used in contracts for years and might be adapted to consumption-based cloud contracting. Standard government invoicing and payment provisions, which are often found in pro-forma "Section G" clauses of the contract, may need to be readdressed to include more specific terms on usage notifications, limits, and credits. Regardless of the types of contracts used to acquire cloud services, it is likely to be the terms and conditions that matter most. Agencies must learn that designing good contract agreements for cloud services involves more attention to the details of terms and conditions ("Ts&Cs"). Those Ts&Cs that are traditionally relegated to "boilerplate" sections of the contract (such as Inspection & Acceptance and Invoicing and Payment) may need to be established as performance requirements within the contract and include more thorough inputs by the program offices and users.

3.3.2.3 How have Cloud Service Providers helped the government in contracting for cloud?

Have CSPs done enough to help the government sort out the best techniques for buying cloud? In general, the session participants were not impressed with what CSPs have done lately. The commercial cloud market is currently so lucrative, it may well be that the big CSPs simply do not feel the need better accommodate government requirements. Instead, the mantra from industry is for the government to embrace more innovative and flexible contracting approaches. Most will not contract directly with the government and prefer to work through resellers to defer risk and performance responsibilities. This does not always work well for the government. One session participant commented that "there are a lot of resellers out there who will promise the moon, but don't come through when push comes to shove." Resellers may be too small to "own the problem" and everything may ultimately come down to the service levels and terms of service offered by the CSPs. Value-Added Resellers (VARs) must also weigh many business considerations in getting certified by CSPs and maintaining their VAR status.

Aside from VARs, have traditional government contractors – the big system integrators (SIs) – stepped up to partner with CSPs to offer value-added services for government needs? Session participants noted some efforts on the part of the big SIs to provide technical services such as program and project management, but not much in the area of business accounting needs such as billing and performance reporting. Similar to SIs, "cloud brokers" have been conceived as a means to outsource cloud service management and absorb risks from the government. Some agencies have moved in this direction but much work remains to be done.

Validating performance of cloud service delivery was raised as a potential area of concern. "CSPs need to do more to ensure that their subcontractors and resellers can perform the jobs contracted for." There was some discussion on the need to obtain credible past-performance data on CSP and resellers. Contract portals, such as those offered by NASA's Solutions for Enterprise-Wide Procurement (SEWP) contract vehicle, may provide a mechanism for such performance information. Participants also noted some evidence of "cloud washing" by prime contractors in which proposed services are vaguely associated with cloud offerings, but do not technically meet the definitions of the National Institute of Standards and Technologies (NIST) [6]. In establishing new vehicles for cloud services, the General Services Administration (GSA) is working with NIST to redefine the definitions of cloud as-a-service offerings (i.e., IaaS, PaaS, and SaaS) and to possibly consider self-certifications.

Despite the belief among session participants that CSPs could be doing more to accommodate government contracting needs, there was broad recognition for the level of out-reach conducted by industry in the form of conferences and symposia. Such forums – often free to

government participants – offer an invaluable means of training and sharing of information and best practices. Additionally, CSPs and industry groups are to be commended for developing informative websites and cost comparison tools that may be useful to government officials in evaluating options for acquiring cloud services.

3.3.2.4 Which government contract vehicles are best for cloud? The Acquisition and Contracting for Cloud Services Session was well represented by officials from GSA and NASA, two agencies that have taken the lead in establishing government-wide contract vehicles for cloud services (along with the National Institutes of Health and the Department of Interior). As might be expected, there was no clear consensus on a single best vehicle for contracting for cloud. Session participants from NASA described how customer requirements are systematically vetted and how, in some cases, customers are referred to other agency vehicles that may be more appropriate. Requirements heavy in labor services may better align with GSA Schedules or Government-Wide Acquisition Contract (GWAC) vehicles. Infrastructure requirements may be better suited for the Department of Interior Cloud Foundations vehicle and customers with smaller, short duration requirements may opt to use GSA's 18F vehicles. There was broad consensus that a well-crafted Statement of Work (SOW) is more important than the vehicle used. "It all comes down to asking 'what is your requirement?' " Although industry has consistently called for maximum flexibility in contract vehicles, it is also important that the government adequately define its requirements and the scope of services required.

GSA described efforts to establish a new Special Item Number (SIN) for Cloud Computing under GSA's IT Schedule 70 [9], its efforts to expand its Blanket Purchase Agreements for E-mail and Infrastructure as a Service, and its new "Hallways" initiative. GSA queried the session participants as to what it could do better to facilitate cloud acquisition by its customers. There were suggestions for more agile contracting models for ordering agreements, as well as templates for SOWs and other required documents. One participant expressed concern over the high cost of FedRAMP [3] authorizations (a process administered by GSA) for small businesses. Giving more visibility to acquisition lead time data associated with ordering under government-wide contract vehicles may help customers in determining which vehicles may be most efficient.

3.3.2.5 What are the major compliance areas? Session participants took note of the extensive conference discussions on security requirements and the FedRAMP processes and recent initiatives. For now these are the priority areas for compliance. However, from an

acquisition perspective, the participants noted the recent GAO reports and Inspector General (IG) reports on cloud computing. While GAO currently appears to be emphasizing the modest progress agencies have made in moving to cloud computing, the IGs are taking a less sanguine look at problems of compliance with standards and regulations. For example, the Council of the Inspectors General September 2014 report [2] pointed out agency contracts for cloud computing that failed to include:

- detailed specifications and best practices documentation (e.g. Service Level Agreements, Data Preservation, Non-disclosure Agreements, etc.), and
- FedRAMP authorization requirements.

Further, the IGs found that agencies were not keeping an accurate inventory of cloud systems being acquired. Agency IGs have begun issuing follow-up audit reports using the methodology of the IG Council report and specific compliance findings are emerging. GAO can be expected to begin similar evaluations of agency cloud contracts. Clearly, the recommendations emerging from these and future GAO and IG reports will weigh heavily in shaping agency policies and practices for cloud contracting.

3.3.2.6 Other Areas (e.g., Workforce Training) Workforce training was briefly discussed, but there was little consensus among the session participants that this is an immediate priority. Industry forums, including conferences and symposia, are serving well at the present to address issues and best practices in this rapidly changing and evolving area. Until the nature of problem areas and best practices are better resolved, efforts to establish formal training may be premature. Session participants noted resources of the Defense Acquisition University and workshops at a recent DISA conference may be helpful. Also, the targeted training resources for Delegations of Procurement Authority (DPAs) on the various GWAC websites may be an effective way for requiring activities to obtain real-time training on developing ordering documents for various contracting vehicles.

3.3.3 Important Findings

- The OMB should coordinate with agencies to issue more specific guidance (e.g. Fiscal Year Guidance OMB 300 / Exhibit 53 reporting) on developing business cases for cloud acquisitions, to include new cloud systems and services as well as migration of legacy systems into cloud environments. The guidance should address techniques for RoI analysis and developing IGCEs.

- The Office of Federal Procurement Policy in coordination with the Chief Information Officers Council and Chief Financial Officers Council, should consider issuing guidance on standard terms and conditions (clauses and provisions) on consumption-based billing and invoicing for cloud services. Such guidance should address governance mechanisms to alert government users when usage approaches various thresholds (i.e., "usage alerts") and acceptable practices for reconciling monthly billing over/under-usage and in applying credits.
- In recognition of their value in educating professionals from both government and industry, OFPP should take a more active role in promoting and participating in industry-sponsored forums on cloud computing acquisition. The purpose of this will be to bring a more consistent message to the workforce on policies and priorities.

3.4 Data Interchange in Federated Clouds

The Data Interchange in Federated Clouds session discussed the best practices and potential solutions for data interoperability between government cloud solutions. The goal of the joint session was to outline recommendations for data exchange formats, best practices for sharing data between government owned clouds (along with using cloud computing to facilitate data exchange between government agencies), discuss the challenges and potential solutions to data exchange within different (or hybrid cloud) environments, and identify best practices for using commercial solutions to ensure the security of government data.

The goals of this session included discussions of the following:

- Discuss standards for government data interoperability
- Discuss best practices for leverage cloud computing to facilitate data sharing within the government
- Identify challenges and potential solutions of using commercial solutions for government data
- Identify best practices for data exchange between hybrid cloud environments

3.4.1 Challenges

These discussions identified the following challenges:

- Data Interoperability problems are at the heart of cloud interoperability

- Avoid moving data into the cloud to solve problems with the data
- Cultural resistance to changing the culture and form of data exists
- Education is key to long term solutions – including lawyers, developers and managers (across all levels)

3.4.2 Discussion Summary

The Data Interchange in Federated Clouds session identified several challenges targeted for mitigation. These challenges include security, connectivity, implementation, collaboration, and legal.

The session participants identified security as a continuing challenge. Specifically, the challenges surrounding sharing data between agencies that originate from policy rather than technology. The technology to share data exists but varying policy and security classifications created barriers between agencies. For example, sharing data between the Veteran's Affairs and the Department of Defense (DoD) regarding a recently retired veteran remains challenging.

Connectivity is of particular interest to the DoD, but applies to other agencies within the government. Trusted connections – even internal to an agency – are required to transfer certain information. Connections to external partners are particularly lacking and cause issues when sharing data.

Agencies select or develop different data management technologies that are best suited to their needs. This can lead to a lack of interoperability between the agencies because of their selected or developed technologies. The same solution or framework can be implemented using different technologies.

Collaboration and agreement between government agencies on the most important cloud services, uses, and adoptions is important but often lacking. In order for data to be most effectively exchanged between government agencies, they should agree on the cloud services and migrations that they will support and make available. For example, date formats and string comparison and handling are both issues on which interoperable systems should agree.

Legal challenges continue to exist within government cloud computing. Some laws prevent cloud migration and data sharing. Further, data security and safety precautions are pre-requisites for any cloud migration, sometimes prohibiting agencies from adopting cloud computing.

The conversation then shifted to discuss digital rights management and the need for trust when storing data within the cloud. It is important to identify the system of record for each piece of data, as well as determine how much of an agency's data is a government record. As such, data *provenance* becomes metadata that is as important as the data, itself. Federated systems should identify the system or program of record, peer data, as well as any metadata required to establish trust of the data and provisioning agency. Digital rights management is influenced by data ownership (is the data government record?) and importance. However, the signing authority is currently unknown (e.g., which agency's key is used?), and a model for data signing in federated systems should be developed.

As government agencies migrate from stovepipe solutions to either internal or external clouds. However, this does not alleviate the responsibility of data management from the owning agency. However, this migration can potentially help establish standard abstract programming interfaces (APIs) that other external services can use for data extraction and consumption. These models can benefit from leveraging and adapting best practices from commercial industry.

Finally, the details of inter-cloud access are challenging. For example, how can a common set of usernames and passwords be managed effectively across the government? Can 3rd-party or open source tools be used to help manage the data interfaces? Commercial practices and solutions can help manage these challenges, but the selection, agreement, and adoption of such practices remains a challenge of collaboration.

3.4.3 Important Findings

- Establish and agree upon standards for data representation, access, management, and provenance
- Remove stovepipes to better share between agencies (intra-agency, inter-agency, to the public)
- Leverage commercial practices, and potentially services, to help alleviate the management challenges

4 SUMMIT RECOMMENDATIONS

Each collaboration session produced common themes. Primarily, the cultural barriers to cloud adoption are no longer as big of a barrier as reported in previous summits, indicating

that the decision makers and cloud practitioners are beginning to understand the value and challenges of leveraging cloud computing in the government from each others' levels. Further, success stories are beginning to emerge (outside of the fringe cases) of cloud adoption. Processes and policies are being shared, and while these success stories, processes, and policies may be difficult to tailor to new use cases and needs or applicable to all government agencies, they are still indicative of progress within the cloud community.

Cloud adopters recognize the value of identifying quick-wins, adopting agile processes, and migrating to cloud; however, these processes are still amoebic, and have not yet been formally defined in a way that is universally reusable. Finally, acquisition remains a perennial challenge, but advancements are being made toward solutions for budgeting, compliance, contracting, and security.

New challenges are arising, such as the need to educate all levels (e.g., CIO versus cloud engineer) of cloud practitioners of the technologies, processes, and challenges within the entire government cloud landscape. However, these new challenges are evidence of the advancements being made toward cloud adoption and acceptance within the government. The government is also investigating leveraging commercial and community support by way of 3rd-party and open source tools.

Academia can provide strong technical resources and insights into the challenge areas discussed. To alleviate the burden on the government, academics should be included in the planning and research processes to help provide technical input. Qualified cloud practitioners are in high-demand, and universities can help provide access to researchers and work with government to identify high value concepts that can help prepare graduates for government cloud employment.

Working groups should also be held to allow cross-government collaboration and discussion to ensure best practices are shared. Some working groups are in the planning stages across the government to discuss more niche concerns. In conjunction with the ATARC Federal Cloud Computing Summit, specialized government-only working groups should be established to allow specific solutions and government programs to be discussed.

Moving forward, Federal Summits and specialized working groups that help broker the conversation within government and between government, academia, and industry will continue to provide high value impacts for government cloud practitioners.

5 CONCLUSIONS

The July 2015 ATARC Federal Cloud Computing Summit highlighted several challenges facing the Federal Government's adoption of cloud computing. The challenges were not compartmentalized based on the challenge areas at the Summit, but span across the discussions by government cloud practitioners. Specifically, cultural aversions, adopting agile processes, security, acquisition, and migration remain difficulties to overcome. Adopting open-source tools, leveraging templates and success stories, and identifying "quick wins" for piloting or testing in a fail-early model can help mitigate the identified challenges.

While the July 2015 ATARC Federal Cloud Computing Summit highlighted areas of continued challenges and barriers to adoption, the Summit also cited notable advances in mitigating these perennial challenges. Most importantly, the perennial challenges that have traditionally existing within the cloud domain have been alleviated at the Cloud adoption level, but persist at the lower, more specific levels of the cloud domain. For example, practitioners and government officers are becoming more educated and understanding of the benefits of cloud computing, but may still require education on the inner workings of the more specific implementations or processes behind the specialized areas. As cloud computing within the government continues to adopt the strategies and practices of other more mature technological domains, cloud computing can be easier to adopt and advance.

From 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. 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[1].

[1] `http://www.fedsummits.com/cloud/`

REFERENCES

[1] Chef Software, Inc. Chef. https://www.chef.io/chef/, 2015.

[2] Council of the Inspectors General on Integrity and Efficiency. The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative. https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report(1)(1).pdf, 2014.

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

[4] Jenkins. Jenkins, CI. https://jenkins-ci.org/, 2015.

[5] V. Kundra. Federal Cloud Computing Strategy. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf, 2011.

[6] 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.

[7] SoftLayer Technologies, Inc. SoftLayer. http://www.softlayer.com/, 2015.

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

[9] U.S. General Services Administration. IT Schedule 70. http://www.gsa.gov/portal/content/104506, 2015.