FEDERAL CLOUD COMPUTING SUMMIT

JANUARY 13, 2016 | 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 January 13, 2016 in Washington, D.C. in conjunction with the ATARC Federal Cloud Computing Summit.

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

MITRE Chair: Justin Brunelle

Challenge Area 1: Planning for Cloud Migration: Fail Early and Often

Government Lead: Jimmy Jones, DOT
Industry Lead: Greg Mundell, CliQr
MITRE Lead: Howard Small

Challenge Area 2: Cloud O&M: Challenges and Solutions

Government Lead: Sara Mosley, DHS
Industry Lead: Dr. Jeff Wootton, Delphix
MITRE Lead: Mano Malayanur

Challenge Area 3: Architecting Future Clouds

Government Lead: Greg Fritz, U.S. Army
Industry Lead: Adam Alphin, Coupa
MITRE Lead: Duy Huynh

Challenge Area 4: Adapting Cloud to Technology

Academic Lead: Wu Feng, Virginia Tech
Industry Lead: Chet Hayes, Chief Technology Officer, InfoZen
MITRE Lead: Demetrius Davis

Challenge Area 5: Standards & Best Practices for Security and Privacy Management in the Cloud

Government Lead: Joe Paiva, Chief Information Officer, International Trade Administration
Industry Lead: Federico Simonetti, Founder and Chief Technology Officer, Extenua
MITRE Lead: Bob Natale, MITRE

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

Challenge Area 1: Planning for Cloud Migration: Fail Early and Often

Darlene Barnett, DISA; Ira Baron, DOJ; David Charbonneau, EPA; Ravindra Chitnis, IRS; Luis Coronado, Jr., DSS; Stephen Donnelly, EPA; Nicholas Glatz, DCMA; Timothy Grandison, Sevatec; Nick Hill, VA; Peter Jim, Census; Samuel Kidane, DOJ; Jeff Knodel, GovPlace; Andrew Luke, IRS; Jerome Madlock, OPM; Jason March, Natoma; Patricia Meyertholen, ED; Brandon Petersen, VA; David Pizzano, GDIT; John Wernau, VA; Audrey Winston, MITRE

Challenge Area 2: Cloud O&M: Challenges and Solutions

Ryan Fleming, FBI; Gregory Gordon, DSS; Stefan Leeb, NOAA; Connor McCarthy, Sevatec; Craig Nelson, $(ISC)^2$; Brian Seagrave, GovPlace; Kathryn Szot, MITRE; Marla Van Tassel, Army National Guard; Jason White, TSA; Gil Woodard, DHS

Challenge Area 3: Architecting Future Clouds

Michael Cassidy, DOJ; James Dinette, Coupa; Robert Holloway, U.S. Army; Frank Kidd, DOL; Anamaria Matos, ED; Michael Meccia, State; Raj Sood, Delphix; William Stephens, U.S. Navy; Pamela Wise-Martinez, PBGC

Challenge Area 4: Adapting Cloud to Technology

Fred Foster, DSS; Bob Franks, State; Henry Hudson, GSA; Bud Michels, GDIT; Brett Pfrommer, DHS CBP; Jeff Williams, DLA; Gil Woodard, DHS

Challenge Area 5: Standards & Best Practices for Security and Privacy Management in the Cloud

Chris Barnes, DISA; Michael Davis, FAA; Jean Claude Descorbeth, DHS; Jothi Dugar, NIH; Raj Dwivedy, Census; Jennifer Fabius, MITRE; Sandra Giger, NOAA; David Harris, DOI; Tom Housman, GDIT; Mackarthur James, Peace Corps; Shashank Kalra, EPA; Anil Karmel, C2 Labs; Darrell Leeks, FBI; Jacques Malebranche, GSA; Dave Merrill, eGlobalTech; Kim Moore, DSS; Eric Most, Peace Corps; Doug Pruss, DHS CBP; Joe Ramsey, ITA; Thomas Reaves, EPA; Ronald Rice, DISA; Julio Rodriguez, ED; Amelia Rudisill, DISA; Mari Spina, MITRE; Ann Williams, State; Michael Wilson, DHS; Victor Zebron, FAA

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 Computing Summit

FEDERAL SUMMITS

JANUARY 2016
FEDERAL CLOUD COMPUTING SUMMIT REPORT*

April 13, 2016

Justin F. Brunelle, Demetrius Davis, Duy Huynh, Mano Malayanur,
Bob Natale, and Howard Small
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 Federal Cloud Computing Summit, held on January 13th, 2016, included five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions. These collaboration sessions allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss challenges the government faces in cloud computing. The goal of these sessions is to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of cloud computing techniques and best practices within the government.

Participants representing government, industry, and academia addressed five challenge areas in federal cloud computing: Planning for Cloud Migration: Fail Early and Often, Cloud O&M: Challenges and Solutions, Architecting Future Clouds, Adapting Cloud to Technology, and Standards and Best Practices for Security and Privacy Management in the Cloud.

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:

> The perennial challenges (e.g., security, adopting agile processes, cultural issues with acquisition) that have existed as barriers to cloud adoption still exist. However, the challenges are no longer at the level of Cloud in general but instead are at lower, finer grained levels of the process. Training and retaining cloud practitioners is a rising challenge as the government continues to migrate to the cloud. The government should collaborate with academia to help train the next generation of government practitioners along with current staff.
>
> While security remains a primary concern, mitigations and best practices are being developed for cloud migration efforts. This includes identifying suitable candidate services for migration and prototyping in cloud environments. Privacy is becoming an increasing concern for cloud migrations, as well.
>
> Mobile devices, Internet of Things (IoT), and cloud will remain closely connected with each enabling the others. Securing cloud access points (e.g., mobile devices) is essential for cloud migrations.

2 INTRODUCTION

During the most recent Federal Cloud Computing Summit, held on January 13th, 2016, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in cloud computing. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of cloud computing technologies and research in the government. Participants ranged from the CTO, CEO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs) [23]. 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 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 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:

- Planning for Cloud Migration: Fail Early and Often
- Cloud O&M: Challenges and Solutions
- Architecting Future Clouds

- Adapting Cloud to Technology
- Standards and Best Practices for Security and Privacy Management in the Cloud

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

3.1 Planning for Cloud Migration: Fail Early and Often

The *Planning for Cloud Migration: Fail Early and Often* session discussed the challenges of migrating applications to cloud environments. The goal of the joint session, with participants from the government, industry and academia, was to outline the recommendations to address the cultural and technical challenges to migration.

The goals of this session included discussions of the following:

- Ideas for addressing cloud security, portability and availability
- Ideas for increasing cloud adoption within the government
- Identify approaches to assist with migrating applications and data to the cloud
- Identify policies to enable adoption and operation of cloud services
- Identify approaches to mitigating fears associated with trusting a third party Information Technology (IT) provider

3.1.1 Challenges

The collaboration session discussions identified the cloud migration challenges and needs provided in this section. The cultural challenges identified by the participants include:

- Encouraging and fostering leadership buy-in to the concept of migrating mission applications and data to the cloud
- Getting the organization's staff to understand what changes will occur as a result of moving to the cloud and how to affect organizational change management
- Understanding the financial models and the costs of migration, particularly with respect to Return on Investment (ROI) and Total Cost of Ownership
- Determining how federal IT funding needs to change for adopting cloud services, and the appropriate method of funding (or, more colloquially, *color of money*) to be used

- Establishing best practices for leveraging the service utility model and the changes in the Federal Acquisition Regulations (FARs) [2] to accommodate the new model
- Overcoming the loss of direct contact with traditional infrastructure is often equated to loss of control of the applications and the data

The technical challenges identified by the session participants include:

- Lack of a common understanding of the cloud by some decision makers, in terms of what it is, what are its benefits, how it works, and how to implement cloud migration
- Concerns about the security of the applications, data, and the underlying cloud infrastructure
- Concerns about secure connectivity from traditional data centers to the cloud and the time and cost of establishing government-wide connection points, including Trusted Internet Connections (TICs) [13]
- Concerns about the portability of any data moved to the cloud and about establishing an exit strategy to move the data to a different environment if needed
- Insufficient tools and approaches to identifying and analyzing the data to determine the appropriate cloud deployment model
- Lack of tools to optimize applications to take advantage of the characteristics of the cloud
- Lack of processes to leverage shared services not generally available from traditional data centers
- Establishing effective Service Level Agreements (SLAs) with the Cloud Service Providers (CSPs)

The needs and best practices identified by the session participants in this session include:

- Understand the mission first, then determine how the cloud can be used to enable the mission
- Determine the value proposition for the cloud with respect to the mission
- Establish development, test, and production environments in the cloud to streamline the cloud implementation process

- As first steps to cloud migration, consider leveraging Software as a Service (SaaS) offerings to replace existing capabilities as appropriate
- Establish a structured methodology (or templates) for migrating applications and data to the cloud from best practices
- Establish an approach to re-architect applications to leverage the cloud's benefits (e.g., scalability)
- Adopt approaches to high availability and disaster recovery services supported by the cloud
- Develop SLAs that address the government's needs for service operation and performance
- Define expectations for application or CSP downtime and identify, collect, and monitor metrics on performance and security accordingly
- Consider the cloud as an option for data center consolidation
- Consider choosing more than one CSP to minimize implementation and portability risks
- Understand how the cloud is tied to mobility and how the cloud must support mobile users across devices with different form factors
- Leverage Indefinite Delivery, Indefinite Quantity (IDIQ) contract vehicles to streamline the process of buying cloud services
- Collaborate with other government organizations to share best practices and lessons learned
- Provide training and education on using and managing cloud services
- Hire more veterans and provide them the training to participate in cloud migration projects to help pair mission-specific knowledge with technical expertise
- Work with Capitol Hill to foster a Cloud IT Bill to support government-wide cloud implementation projects

3.1.2 Discussion Summary

The *Planning for Cloud Migration: Fail Early and Often* session identified several challenges and needs. For example, the participants identified a primary concern with some government policy makers' limited awareness and understanding about the cloud, especially in terms of service offerings and benefits. Increased awareness will help overcome this, along with other, barriers to adoption. The discussions also re-emphasized the persisting perennial cultural challenge of communicating to government leadership and staff the operation and benefits of cloud computing. Past Federal Cloud Summits have identified limited knowledge of cloud computing among policy makers as a challenge to cloud adoption [6, 7, 8]. This limited understanding of cloud computing often extends to security, particularly with regards to protecting applications, data, and connectivity to traditional data centers.

To aid with cloud migration, the session participants recommend establishing technical approaches and exit strategies to maintain data portability across multiple CSPs. Further, migration strategies should include a structured methodology for migrating applications and data to the cloud, including re-architecting applications and improving availability. However, cloud migration may involve changing the government's acquisition and funding policies along with regulations to enable the adoption of IT services via a utility (or similarly scalable or adaptable) model. As part of this change, the session participants recommend developing SLAs with the CSPs that address the government's needs for service operation and performance. Finally, the session touched on the importance of including other emerging technologies in migration plans.

3.1.3 Recommendations

The participants in the *Planning for Cloud Migration: Fail Early and Often* collaboration session identified the following recommendations, in terms of "quick wins":

- Develop initial proof of concepts in the cloud to increase understanding of how to leverage the cloud and to establish, learn from, and quickly achieve initial implementation successes; this could include building or migrating less complex applications such as small websites or conducting a SaaS pilot to understand how to implement software to replace existing applications
- Stand up development and test environments (i.e., *sandboxes*) in the cloud to improve standardization and streamline the development and testing processes. The environments could be used to provide technical training on building and migrating UNCLASS applications and data.

- Develop approaches to improve understanding of the cloud, especially among government leadership, to establish buy-in and increase adoption
- Establish improved collaboration within government cloud communities to share best practices and lessons learned (e.g., continuing the ATARC Innovation Labs [20]) and use the results of the collaboration to aid the planning and implementation of cloud projects
- Improve the government's understanding of cloud security with respect to the applications, data, and connectivity
  - Include understanding the security responsibilities between the government and the CSPs
  - Specify the sensitivities of the data associated with the applications to determine what cloud models and services would be most appropriate
- Work with the CSPs to develop SLAs to clearly specify government expectations for service operation and performance
- Work with the CSPs to determine strategies for increasing data portability including understanding CSP and third-party technologies for moving data between cloud environments.
- Implementing these "quick wins" may require the government to change funding and acquisition policies and approaches to buying IT capabilities via a utility model

3.2 Cloud O&M: Challenges and Solutions

The *Cloud O&M: Challenges and Solutions* session discussed best practices for operations and end-to-end management for cloud services. The goal of the joint session was to outline recommendations for O&M in different clouds, dealing with commercial CSPs, and evolving current practices to adapt to cloud environments. Further, with the understanding that cloud computing will change and evolve in the future, this session aimed to identify processes that will help O&M evolve along with the cloud technologies.

The goals of this session included discussions of the following:

- Identify best practices for private versus CSP-owned cloud management
- Establish recommendations of O&M process shifts to adapt to future evolutions in the cloud domain

- Evaluate current O&M to understand whether government is taking full advantage of cloud features

3.2.1 Challenges

The collaboration session discussions identified the following *Cloud O&M: Challenges and Solutions* challenge areas or needs:

- Lack of a broad, general cloud based reference architecture that weaves together the various cloud service offerings (Infrastructure, Platform, and Software, or IaaS, PaaS, and SaaS) and cloud deployment models (Private, Public, Community, and Hybrid) to best meet the requirements of the agency
- Need for a change in culture, including organizational change, change in policy including perhaps the law, and the need for training and education for government practitioners
- Need for a catalog of cloud service providers and their offerings with a sufficient level of granularity of service offerings and approaches to increase the portability between cloud computing provider environments

3.2.2 Discussion Summary

The *Cloud O&M: Challenges and Solutions* session identified several challenges regarding the process of adopting cloud computing and managing cloud services once adopted. Also discussed was the potential impact of inaction on existing applications or processes that should be migrated to a cloud environment. Participants recommended policy and potentially legal incentives (from the Office of Management and Budget (OMB))for migrating to cloud environments where appropriate. The *silo* culture within the government is a potential barrier to cloud adoption and cost sharing; a cloud reference architecture that demonstrates the operation, value, benefit, and potential path to cloud adoption would help alleviate the cultural barriers to operating in a shared environment.

Cloud environments are operationally and technically complex, making control and management a greater challenge. This is increasingly difficult when dealing with multiple CSPs or deployment models (e.g., private, public, hybrid). Establishing, collecting, and *tracing* comparable metrics for cloud usage is difficult in these heterogeneous cloud environments. Traceability is essential for performing the billing and acquisition categorizations – or binned models – recommended by some of the other summits and sessions. From these derived

bins of cloud usage and needs, the government can establish more effective configuration management for improved logging, monitoring, and control. This will further aid with cultural resistance and risk-aversion to cloud migration due to the accountability-control imbalance between government agencies (which assume all accountability) and CSPs (which control the services).

Open source technologies can also help mitigate some of the management and budgetary challenges of cloud adoption. Open source tools are often suitable for cloud services and can be adopted by cloud consumers to help facilitate data and service portability (e.g., to avoid vendor lock-in[1]) and can be included in SLAs to ensure their continued support.

The session participants also recommended that the Cloud Security Alliance (CSA) help establish improved roles and responsibilities for government cloud adoption. For example, the complex relationships between CSP, consumer, and broker may create contractual challenges for which the CSA makes neither deployment model nor service recommendations. Identity access management and Federal Information Security Modernization Act (FISMA) [12] compliance are also challenges in cloud environments that have complex relationships between stakeholders.

Mandated cloud adoption becomes additionally challenging when considering the Department of Defense initiatives (e.g., the Joint Information Environment (JIE) [9] and Mission Partner Environment (MPE) [11]). Specifically, FedRAMP [15] control does not yet consider OCONUS[2] private and hybrid cloud environments.

3.2.3 Recommendations

The *Cloud O&M: Challenges and Solutions* collaboration session participants identified the following recommendations:

- Cloud adoption is still a challenge due to lack of architecture guidelines at the required levels of granularity
- Significant cultural barriers exist to cloud adoption that should be addressed through a combination of legislation, OMB directives, education, and training
- Clarity is required on how a complex cloud environment is to be managed, including clarity of the roles and interoperability between cloud environments

[1] Alternatively, session participants recommend brokering technologies can be employed to help facilitate charge-back and avoid challenges from vendor lock-in.

[2] Outside of the continental United States.

3.3 Architecting Future Clouds

The *Architecting Future Clouds* session discussed how the government can best prepare for the next disruptive cloud technology. The goal of the joint session was to outline methods of predicting and adopting new technologies in the cloud domain and identifying ways in which the government can help direct research to develop the next era of cloud computing.

The goals of this session include discussions of the following:

- Identify methods of adapting to new emerging technologies in the cloud
- Propose methods for government cloud practitioners to use when preparing for the evolution of the cloud technologies
- Recommend methods the government can use to influence academic and industry research and development of cloud technologies

3.3.1 Challenges

The collaboration session discussions identified the following *Architecting Future Clouds* challenge areas or needs:

- Government agencies – in general – do not have cloud researchers on staff
- Department of Defense agencies tend to have issues with low bandwidth, at-the-edge, isolated remote networks, multi-tendencies, and use Storage or Software as a Service
- Procurement process is not yet optimized for getting the best bang-for-the-buck instead of just getting the best price
- Classification and segmentation of data and moving non-classified data onto cloud platforms remains a challenging process
- Challenging environments with limited service (e.g., Disconnected, Interrupted, and Lossy (DIL) environments) reduces the agility for new cloud services to be implemented
- Security concerns with some government community clouds are being targeted because they stand out[3]
- FedRAMP bottlenecks introduce challenges when not connected to clouds

[3] That is, government only clouds reduce the attack surface of malicious agencies, identifying government cloud systems by default.

- SLAs are often overlooked if inadequately defined or even left omitted from requirements
- Commonly, systems are not baselined before migration to cloud environments, making measuring benefits more difficult
- Cloud computing for OCONUS is challenging and not well defined
- Lock-in is still possible when using proprietary software
- Data portability and open standards for software in the cloud communities remains challenging (not only within government adoption)

3.3.2 Discussion Summary

The initial direction of the *Architecting Future Clouds* session discussion was to define the scope of what pertains to the cloud and the areas in which the participants operate[4]. The three key areas that refer to the scope of the cloud discussion are:

1. Government Community Cloud
2. Public Cloud
3. Hybrid Clouds

The participants mentioned a desire for more products to be provided as a service instead of traditional product offerings. They also agreed the future is in the mobile realm as applications increasingly move towards mobile platforms; mobile devices often offload computationally intensive operations to clouds. The participants recommend using the agile processes[5] to help create an organization with increased agility and that enables frequent new releases of their services. The consensus for migrating towards adopting cloud technology for the government is to transition to a community cloud and eventually move towards a public cloud. One of the major hurdles for adopting cloud technology is it's vastly increased complexity over previous technologies due to the many things it covers leading to expanded adoption timelines. Cloud implementation processes continue to struggle with security,

[4]For example, the Department of Education focuses on providing services to students and financial aid across the Universities across the US; the Department of Labor works with pensions, minimum wage fraud, sensors in mine, users in the field doing investigations; the Department of Justice has few enterprise services, commoditized services, manageable SaaS, security, procurement.

[5]The agile processes that can benefit cloud adoption include fail-early models to identify best practices and increased feedback from end users and stakeholders.

procurement, training, and the need for culture change – all perennial challenges with cloud adoption. There needs to be a culture change from top-to-bottom in organizations for cloud technology adoption.

3.3.3 Recommendations

The *Architecting Future Clouds* collaboration session participants identified the following recommendations:

- Research automated data classification
- Training of decision makers, engineers, and other cloud practitioners to be more aware of advances in cloud technologies
- Start with small cloud adoption projects by putting unclassified data into the public cloud instead of further delaying the transition to cloud technologies with larger challenging migrations
- More research and development is needed for projects that differentiate between data types (classified data, non-classified) to help data that needs to be parsed and be placed in the appropriate environment, allowing more data to be placed on the public clouds instead of creating a private or hybrid cloud
- Migration towards the public cloud should be the primary goal of government agencies except for portions of the Department of Defense and Intel Community (which will stay on the community cloud due to inclusion of sensitive data)
- To progress towards adopting cloud technologies there must be movement towards utility computing
- SLAs need to be incorporated early on and vetted when moving over to the cloud environment
- Future cloud architectures should be defined for every element down to the end-user
- Cloud adopters should consider having reserve funds in a pilot project to adapt to new technologies
- Cloud adopters should review prior adoption efforts and select the most successful and lessons learn and adapt that towards future projects and task

3.4 Adapting Cloud to Technology

The *Adapting Cloud to Technology* breakout session was attended by a diverse group of thought leaders representing several defense and civilian agencies as well as industry and academia. The group, comprised of experienced IT professionals, quickly zeroed in on key strategic and programmatic challenges that impede their organizations' ability to realize the cloud's elusive promise of cost savings, efficiency gains and an "on-demand" IT infrastructure. A few discussion points were presented to the group to ensure sufficient breadth in the group's deliberations and session report.
The goals of this session included the following:

- Identify opportunities for leveraging emerging technologies (e.g., mobile technologies, the IoT) to support cloud models (e.g., hybrid, private, public clouds)
- Identify trends of cloud adoption to support emerging technologies
- Identify current challenges with networks and connectivity limiting cloud-enabled emerging technologies
- Make recommendations for the role of cloud computing in technology refresh cycles

3.4.1 Challenges

The collaborative session generated a number of challenges to adapting cloud computing technologies and services to current and emerging technologies. Below is a summary of the major pillars of obstruction:

- The government's biggest cloud challenges are not technology-related – cultural changes are needed to cut through bureaucracy and inhibiting IT personnel, policies and practices
- Fear of the unknown impedes the government's ability to identify and assess applicable risks and threats despite the presence of mitigating technology solutions or business process changes; this fear also inhibits fruitful partnerships and open communications between government and industry
- Large IT modernization initiatives often lack adequate buy-in, support from leadership and is difficult to financially justify significant IT infrastructure changes in the face of rapid technology changes and constrained IT budgets

- Most medium to large IT enterprises commonly struggle with consumer technology insertion (e.g., the mobility market is tailored to the needs and wants of the individual user vice the enterprise) and the utility (or, more colloquially, *pay by the drink*) model employed by CSPs. Adapting to these new paradigms may lead to administrative and management issues for public sector customers
- Budgeting and acquisition processes and policies incline organizations to seek a "one size fits all" approach or solution
  - Conversely, cloud service models enable unprecedented agility for organizations to address specific operational use cases involving mixes of user groups, technology and security requirements, geographic regions and usage patterns
  - There is often a lack of understanding and expertise within the government users and decision makers to successfully bridge these divergent business models

3.4.2 Discussion Summary

The group discussion was intended to examine the session topic from the perspective of current technologies, emerging technology trends, as well as current interoperability models employed within the federal government.

- What impact will IoT and mobile integration into clouds have on FedRAMP and other cloud security practices?
- Should cloud practices adapt to support other emerging technologies?
- How should the government plan to adapt their clouds to prepare for future emerging technologies?
- How can the government leverage other emerging technologies (e.g., IoT, mobile) to support cloud models (e.g., hybrid, private, public clouds)? How is cloud impacting the adoption of emerging technologies?
- How can networks (government-only and commercial) adapt to enable cloud interoperability?
- What is the role of cloud computing in the technology refresh cycle?

Identifying challenges was a far easier task for the session participants than articulating possible remedies to said challenges. The dearth of success stories validated the difficulty agencies have encountered in enhancing and extending their existing IT infrastructures and applications with cloud-based capabilities.

The group targeted the cultural impediments with clear, actionable ideas. For example, rather than petitioning leadership to move everything to the cloud, session participants expressed ways to help the government adapt to and implement new technologies, market shifts, standards, and best practices. Another idea was to effectively manage risk and complexity with proven, trusted techniques as to combat fears of the unknown or the different. Many security-focused policies institutionalize these fears and prevent government and industry partners from working through actual security and implementation concerns.

Another round of discussion examined the "hows" of modernizing and extending existing IT infrastructures to support current and emerging technologies such as IoT, virtualized desktops, and mobility services. Organizational role and responsibility challenges such as data ownership, access control, and reciprocity were also noted as outstanding actions for the federal government IT community.

3.4.3 Recommendations

The *Adapting Cloud to Technology* collaboration session participants identified the following recommended first steps toward a more widespread adoption and execution of the Federal CIO's "Cloud First" policy [14]:

- Learn to "order from the menu" whenever possible (i.e., leveraging existing models)
- Talk goals and outcomes with vendors – not just "mission requirements" and policy compliance
- Understand that customized, hard-to-integrate solutions have short ROI, long maintenance tails
- Re-look and revamp business processes (e.g., governance, acquisition, management) related to cloud, mobile, and emerging technologies
- Consumer-based technologies are evolving too fast for current set of government policies, processes
- Changes must originate from the top and align with industry trends, standards, and best practices

- Commit to continuous education, modernization to stay within one generation of market leaders
- Strategic planning and analysis are needed before any mass migrations to cloud
- Thoroughly assess portfolio before forklifting apps, data to the cloud
- Use tech refresh cycles as opportunities to evaluate, re-engineer major IT systems
- Learn to be risk-tolerant instead of risk-averse

3.5 Standards and Best Practices for Security and Privacy Management in the Cloud

The *Standards and Best Practices for Security and Privacy Management in the Cloud* session extended discussions of cloud security conducted at previous Federal Summits by focusing on current challenges in cloud security and privacy protection, relevant standards and best practices, and related challenges unique to government community clouds.

Reflecting the range of concerns associated with the session topic, a relatively large set of concerns was posited for discussion, including:

- What standards and best practices (existing or in progress) support security and privacy management in the cloud?
- How sufficient is the growing set of NIST guidance on cloud computing?
  - NIST SP 500-291: Cloud Computing Standards Roadmap [21]
  - NIST SP 500-292: NIST Cloud Computing Reference Architecture [18]
  - NIST SP 500-293: US Government Cloud Computing Technology Roadmap Volume 1, High-Priority requirements to Further USG Agency Cloud Computing Adoption [4]
  - NIST SP 500-293: US Government Cloud Computing Technology Roadmap Volume II, Useful Information for Cloud Adopters (Draft) [1]
  - NIST SP 500-293: US Government Cloud Computing Technology Roadmap Volume III, Technical Considerations for USG Cloud Computing Deployment Decisions (Draft) [3]
  - NIST SP-500-299: NIST Cloud Computing Security Reference Architecture (Draft) [22]

  - NIST SP-800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations [not specific to clouds, but important to the discussion topic] [10]
  - NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, [17]
  - NIST SP 800-145: The NIST Definition of Cloud Computing [19]
  - NIST SP 800-146: Cloud Computing Synopsis and Recommendations (Draft) [5]

- How do the NIST "essential characteristics" of cloud computing affect security concerns and management?
- How will the FedRAMP High Baseline [16] and TIC support facilitate high impact application implementation in the cloud?
- How does security control inheritance work in cloud service and deployment models?
- What special benefits in the security and privacy domains do government-only community clouds provide?
- How does shared responsibility for security affect the Security Operations Center (SOC) mission (organization, performance, SLAs, cost, etc.)?
- What about shared responsibility for privacy, particularly beyond the aspects of privacy that that relate to security (e.g., what does a CSP need to provide to ensure an agency can adequately complete a Privacy Impact Assessment (PIA), or when facing a privacy breach in the cloud)?
- What unique security and privacy weaknesses, vulnerabilities, threats, exploits, and defenses apply to cloud computing and how are they best mitigated?
  - Enterprise: Collateral contamination of cloud provider or other user data
  - "Hybrid" (above, plus): Indices may be inverted, contaminated
  - Cloud provider response to consumer requirements to find personally identifiable information (PII) needed for requests (e.g., Privacy Act, Freedom of Information Act (FOIA), e-discovery requests)
  - Lost or corrupted PII by cloud provider
  - PII stored outside a US jurisdiction (foreign laws, redress)

  - Law enforcement access without notice (Electronic Communications Privacy Act (ECPA) standards for stored data)
  - Data retention and cloud provider rights to data (e.g., "perpetual" licenses, use, deletion)
  - Disposition of PII at the conclusion of service

- Are the CSA defined categories for Security as a Service complete as currently documented (individually and collectively)?
- Does the CSA correctly identify and describe the critical areas of focus in cloud computing and does its security guidance in these areas facilitate successful implementations?
- Are useful Security as a Service offerings available and how can they be leveraged by government cloud applications?
- How will software-defined everything (and especially software-defined networking (SDN)) impact security and privacy management in the cloud?
- Security challenges and potential mitigations to software-defined networks that utilize cloud services?
- What special concerns does the IoT raise for security and privacy management in the cloud?
- How can identity, authentication, authorization, and access control be most effectively managed across cloud service and deployment models?
- How do cloud-based key management systems compare to on-premises alternatives?

The actual session discussion was not constrained to these planned topics; participants were free to raise and pursue additional topics of interest.

3.5.1 Challenges

The collaboration session discussions identified the following challenges that might be solved and needs that might be met by applying existing or developing new *Standards and Best Practices for Security and Privacy Management in the Cloud*:

- Application readiness assessments:

  - How to determine whether an application is appropriate for the cloud, using which service and deployment model(s)?

- Data-centric security approach:
  - Data ownership, validation, or governance?
  - Data encryption/decryption and key management over diverse and dispersed storage resources?
- Integration of hybrid environments (IoT, laboratory equipment, medical devices, etc.):
  - Device security controls and processes in a hybrid government furnished equipment (GFE) equipment environment:
    * Device access rules
    * Device health checks
    * Device limitations (GFE vs non-GFE)?
- Control of CSP customer portal user accounts:
  - Controlling access to credentials (e.g., administrators, account owners)?
- Private key infrastructure (PKI) authentication over Transport Layer Security (TLS) v1.2 with Perfect Forward Secrecy (PFS) (and client cert authentication)?
- Need for user authorization best practices (especially for privileged users)?
- Firewall configurations to manage highly mobile or transient access to cloud-based applications (e.g., database-as-a-service):
  - Data criticality/value
  - Decision tree in the Enterprise Architecture
- Distinctions between civilian and defense segments of US Government (e.g., differences in Identity and Access Management and authorization practices)?

3.5.2 Discussion Summary

Candidate solutions – some existing and some novel – to a number of the challenges discussed (per above) were identified by the participants in the group discussion. In some cases, rather

than candidate solutions, the discussion identified the need for additional information, testing, and so forth.

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

- The need to clearly understand the distinctions among particular cloud service offerings (e.g., computing as distinct from storage in IaaS) and the interrelationships among them
  - And any associated special considerations depending on cloud service models (IaaS, PaaS, SaaS, XaaS) and cloud deployment models (public, private, community, hybrid)
- The need to understand CSP privacy practices (beyond confidentiality controls)
  - The recognition that government security staffs are stretched thin; CSPs are likely better staffed and, on the whole, have more mature security and privacy practices
  - Insufficient knowledge of cloud/CSP security and privacy possibilities
- The potential role of network segmentation
  - Especially in hybrid cloud implementations
  - Especially the emerging software-defined perimeter (SDP) approach[6]
- The need to promote cooperation between CSPs and Independent Software Vendors (ISVs) concerning authentication (authN) and authorization (authZ) standards and best practices
  - Privileged access workstations
  - Single Sign-On (SSO), e.g. from DHS native ID passing to CSP
  - Federated ID management
  - Two-factor authentication
- Centralized management of data access policies – independent of authentication (i.e., support multiple authN schemes).
- The potential role of Cloud Access Security Brokers (CASBs)
  - Provide centralized CSP-agnostic security rights systems

[6] Refer to `https://cloudsecurityalliance.org/group/software-defined-perimeter/`.

  - CASBs are on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement[7]
  - Minimal evident adoption and utilization of the CASB role in the marketplace as of yet

- The need to understand (and possibly modify) application architecture as part of, or as a result of, application readiness assessment for cloud migration

  - Some applications can be migrated but retain the need to access local data (hybrid cloud)
  - Many systems are not modernized (even pre-cloud levels)
  - Re-architecting some applications (e.g., to leverage microservices) might be necessary
  - The decision tree should include all specific functionalities provided by or needed by the application
  - Maybe it is better to not move things that are not ready?
  - If the application uses structured storage, then perhaps the application and its data should be deployed together (i.e., on the same infrastructure)

  The sense of the discussion was more exploratory than declarative; in other words, all of these observations were raised as considerations or possibilities for assessment, tailoring, extension, and so forth, as each case might warrant. The discussion tended to highlight the fact that while the set of possible concerns is not small (and perhaps not even fully identified as of yet), viable solutions either exist or can be assembled.

3.5.3 Recommendations

The participants in the *Standards and Best Practices for Security and Privacy Management in the Cloud* collaboration session identified the following important findings and recommendations:

[7] Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection, prevention, and more. See `http://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs` for additional information.

- The government needs an all-star team of FedRAMP, NIST, DISA, DHS, and industry to collaborate or a consolidated and actionable set of standards and best practices for security and privacy management across all cloud service and deployment models
- A solid foundation already exists among the various guidance documents produced thus far, but it needs to be distilled into a more manageable set – perhaps by application type profiles – for realistic acquisition and implementation processes
  - The NIST online resources might provide a workable venue for such collaboration[8]
  - A greater focus and emphasis must be placed on protecting the data (e.g., slicing, replication, distribution) as a primary element of application readiness assessment for cloud migrations
- Mobile, specialized devices, and IoT will be key to accessing the cloud going forward; therefore, reliable security and privacy mechanisms for those devices and access paths must be devised up front
- Mobile Device Management needed for mobile and analogous solutions needed for other specialized devices that will access the cloud
- SDP technology must be aggressively explored and fitted to cloud service and deployment models for security boundaries via network segmentation
- Trusted cloud credential management/managers are needed – leveraging IdAM, role-based (RBAC), and attribute-based (ABAC) access control – especially for cloud administration/privileged user accounts
  - CSABs might contribute to a solution on this front
  - Need to protect against insider threats in CSP environments
  - Need to integrate government-controlled trusted certificate authorities
  - Need for tiered access control solutions, especially in hybrid cloud deployment models
  - Need better tools for application migration suitability assessment and for automating migration activities

[8] Please refer to `http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome`, `http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity`, `http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/FederatedIdentityInACloudEcosystem`, and `http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/ApplicationContainersAndMicroservices`

- Need to unify CSP management efforts, to drive vendors toward:
  - Unified (or at least uniform and interoperable) management systems
  - Support for customer data management policies
  - Support for customer authentication, authorization, and access control rules
  - Support for customer-configured sage tracking and reporting

The challenge area discussion group recognized that government policy, technology evolution, and IT economics mandate greater use of cloud services. At the same time, despite major progress among CSPs (promoted by FedRAMP compliance), some hurdles remain on the security and privacy management front. Those hurdles can be removed or substantially lowered via well-constructed standards and field-proven best practices. Identification of specific needs is a first step toward such a solution and, it is hoped, the discussion outcomes as reported here serve as that first step.

4 SUMMIT RECOMMENDATIONS

As with past Federal Cloud Summit discussions, the collaboration sessions discussions had a common set of themes. While the cultural barriers to adoption, lack of training and technical understanding, and security (better known as the perennial challenges of government cloud adoption) remain, mitigations and success stories are emerging from government adoption efforts. With continued collaboration and sharing, establishing success stories and best practices is becoming more common-place and cloud adoption is becoming easier for government agencies. While the perennial challenges still persist, they are becoming more manageable due to the various mitigations arising.

CSPs are adopting practices that make government cloud adoption easier, including facilitating acquisition and improving security. This extends to emerging technologies such as IoT and mobile devices. Securing the cloud access points will help improve cloud adoption and security. The government still recommends using agile processes and identifying UNCLASS targets for cloud migration as the best initial steps for beginning cloud adoption.

Some interesting points were raised in the discussions, as well. For example, government-only cloud environments limit the target frontier for malicious agents. As such, public clouds may provide a benefit over government-only clouds for the proper migration targets. Further, cloud adoption may be inhibitted by risk aversion, particularly when beginning the cloud migration and acquisition process. Calculated risks during adoption can help

facilitate leveraging the cloud; the government should encourage or enable calculated risks with appropriate rewards as a way to mitigate risk aversion with cloud migration.

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 formed to allow cross-government collaboration and discussion to ensure best practices are shared. Some working groups (e.g., the ATARC innovation Labs) are being implemented across the government to discuss more niche concerns. In conjunction with the 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 January 2016 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, securing cloud access points, and acquisition models remain difficulties to overcome. Leveraging emerging technologies, leveraging success stories and best practices, and identifying "quick wins" for piloting or testing in a fail-early model can help mitigate the identified challenges.

While the January 2016 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, these challenges that have traditionally existed 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, CSPs are introducing practices that facilitate government cloud adoption. 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.

Based on the recommendations made in the Collaboration Sessions, government practitioners (at all levels of government) should participate in special interest groups or working groups to increase collaboration; continue to influence standards development within the discipline; and continue to partner with academia to leverage cross-cutting research and to help train the government workforce. 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[9].

REFERENCES

[1] Us government cloud computing technology roadmap volume ii, useful information for cloud adopters. Technical Report Special Publication 500-293, National Institute of Standards and Technology, 2011.

[2] Acquisition.gov. Federal acquisition regulation (far). `https://www.acquisition.gov/?q=browsefar`, 2016.

[3] L. Badger, D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf. Us government cloud computing technology roadmap volume i release 1.0. Technical Report Special Publication 500-293, National Institute of Standards and Technology, 2011.

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

[4] L. Badger, R. Bohn, S. Chu, M. Hogan, F. Liu, V. Kaufmann, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf. Us government cloud computing technology roadmap volume ii release 1.0: Useful information for cloud adopters. Technical Report Special Publication 293, National Institute of Standards and Technology, 2011.

[5] L. Badger, T. Grance, R. Patt-Corner, and J. Voas. Cloud computing synopsis and recommendations. Technical Report Special Publication 800-146, National Institute of Standards and Technology, 2012.

[6] 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.

[7] 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.

[8] 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.

[9] Defense Information Systems Agency. Joint Information Environment. `http://www.disa.mil/about/our-work/jie`, 2016.

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

[11] Department of Defense. Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD. Technical Report 8110.01, Department of Defense, 2014.

[12] Department of Homeland Security. Federal information security modernization act (fisma). `https://www.dhs.gov/fisma`, 2016.

[13] Department of Homeland Security. Trusted internet connections. `http://www.dhs.gov/trusted-internet-connections`, 2016.

[14] Federal CIO. Federal cloud computing strategy. https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf, 2011.

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

[16] FedRAMP PMO. FedRAMP High Baseline. https://www.fedramp.gov/provide-public-comment/fedramp-high-baseline/, 2015.

[17] W. Jansen and T. Grance. Guidelines on security and privacy in public cloud computing. Technical Report Special Publication 800-144, National Institute of Standards and Technology, 2011.

[18] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf. Nist cloud computing reference architecture. Technical Report Special Publication 500-292, National Institute of Standards and Technology, 2011.

[19] 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.

[20] G. Mundell, K. Jones, and V. Subbiah. Atarc cloud innovation lab. http://www.atarc.org/innovation-labs/cloud/, 2016.

[21] NIST. Nist cloud computing standards roadmap. Technical Report Special Publication 500-291, Version 2, National Institute of Standards and Technology, 2011.

[22] NIST. Nist cloud computing security reference architecture. Technical Report Special Publication 500-299, National Institute of Standards and Technology, 2012.

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