# FEDERAL CLOUD COMPUTING SUMMIT

JANUARY 14-15, 2015 | 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 14, 2015 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:

**Challenge Area 1: When to choose Public, Private, Government, or Hybrid clouds?**

Industry Lead: Scott Chapman, Project Hosts
MITRE Lead: Karen Caraway

**Challenge Area 2: The umbrella of acquisition: Contracting pain points and best practices**

Government Lead: Stan Kaczmarczyk, GSA
Industry Lead: Domenic Cipicchio, Deloitte
MITRE Lead: Michael Kristan

**Challenge Area 3: Tiered architecture: mitigating concerns of geography, access management, and other cloud security constraints**

Industry Lead: Mark Odell, CGI Federal
MITRE Lead: Nicole Gong

**Challenge Area 4: The role of cloud computing in emerging technologies**

Industry Lead: Dominic Delmolino, Agilex
MITRE Lead: Nancy Ross

In addition, I would like to recognize two individuals whose efforts contributed to the success of this program: MITRE Lead Justin Brunelle and ATARC Lead Tim Harvey.

And finally, thank you to all government, academic and industry members who participated in these dialogue sessions. Without your Cloud Computing knowledge and insight, this White Paper would not be possible.

Sincerely,

George Thomas Suder

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

# January 2015 Federal Cloud Computing Summit Summary

*Karen Caraway, Nicole Gong, Michael Kristan, Nancy Ross, Justin F. Brunelle*
*The MITRE Corporation*

*Tom Suder*
*The Advanced Technology Academic Research Center*

## Abstract

The latest installment of the Federal Cloud Computing Summit took place on January 14th-15th 2015. The Summit began on January 14th with the MITRE-Advanced Technology Academic Research Center (ATARC) Collaboration Sessions that allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss the government's challenge areas in cloud computing. The goal of the collaboration sessions is to create a forum for an exchange of ideas and a way to create recommendations to further the adoption and advancement of cloud computing within the Government.

The MITRE Corporation 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. MITRE worked in partnership with the ATARC to host these collaborative sessions as part of the Federal Cloud Computing Summit.

The collaboration sessions occur on the first day of the two day Federal Cloud Computing Summit. On January 15th, Maria Roat (Chief Technology Officer of US Department of Transportation) gave the opening keynote. The Summit continued with a series of panel discussions, an industry trade show, and concluded with a panel discussion on the collaboration session outcomes. The goal of the collaboration sessions is to create a forum for an exchange of ideas and a way to create recommendations to further the adoption and advancement of cloud computing within the government.

The goal of the MITRE-ATARC Collaboration Sessions is to enable the collaboration between government representatives that potentially would not otherwise meet, academics, and industry representatives. The sessions identify challenges, best practices, recommendations, success stories, and requirements to further the state of cloud computing in the government.

The government, industry, and academia met 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 hire-ready graduates to advance the state of cloud computing in the government.

Several recommendations were made as a result of the exchange of ideas in the collaboration sessions. This white paper summarizes the discussions in the collaboration sessions, as well as identifies recommendations for government and academia while identifying orthogonal points between challenge areas. It also recommends an increase in cross-government and academic collaboration to share best practices and address cross-cutting challenges.

This paper elaborates on the following high-level outcomes:

- Many perennial challenges in cloud computing persist (e.g., acquisition, security, vendor lock in), but are being mitigated
- The "true cost of adoption" and return on investment calculations should include standard units of cost, quantifiable metrics, and should measure the cost of delayed adoption
- Agile processes (e.g., fail-early models, rapid deliveries) can help mitigate risk during cloud adoption

## Collaboration Session Outcomes

At the collaboration symposium, participants broke into four separate collaboration sessions with each session discussing a different challenge area. Each MITRE-ATARC Collaboration Session was a focused and moderated discussion among government, industry, academic, and MITRE representatives about a cloud computing challenge area.

Four separate sessions were held, individually focusing on:

- Public, Private, Government, or Hybrid clouds?
- The Umbrella of Acquisition
- Tiered Architectures
- The Role of Cloud Computing in Emerging Technologies

Participants discussed current problems, gaps in work programs, potential solutions, and ways forward for each of the challenge areas. This section outlines the goals, outcomes, and a summary of each of the collaboration sessions.

### *Public, Private, Government, or Hybrid clouds?*

The Public, Private, Government, or Hybrid Clouds session discussed the unique challenges, benefits, and policies associated with different categories of cloud deployments available for government adoption. The goal of the joint session was to outline recommendations for how to select the appropriate cloud for implementation and adoption, as well as identify the best practices for adoption.

The goals of this session included discussions of the following:

- Identify which categories of cloud the government should adopt under what conditions
- Identify the unique challenges and benefits of each cloud category
- Discuss best practices for adopting a hybrid cloud approach

- Recommend policy changes to increase the ease of hybrid cloud creation and adoption

The discussions identified the following needs:

- Reform of acquisition policy to facilitate the cloud computing utility model necessary for predictive pricing
- Establish government/organization cloud broker to streamline and standardize cloud requirements and procurements
- Leverage lessons learned from other government cloud adopters to avoid delays during cloud adoption and use
- Using agile processes, start small and utilize least restrictive deployment models that meet the needs of the organization
- Launch a fundamental shift in organization culture and business processes required for successful cloud computing adoption
- Increase cloud computing education with emphasis on colloquial rather than scientific terms

The summary of the collaboration session is below:

The Public, Private, Government, or Hybrid Clouds session identified several challenges targeted for mitigation. Significant time was spent discussing the cloud deployment definitions. It became apparent that the collective perceived definitions of public, private, government, and hybrid clouds did not align with the NIST definitions[1]. The NIST cloud definitions are too scientific for the non-technical consumer to understand and therefore further clarification and education among the potential cloud community is required. Therefore, the attendees agreed to high-level definitions based on use of the deployment models based on availability:

- Public – All users
- Private – Limited set of users
- Community – Restricted set of users
- Hybrid – Combination of Public, Private, Community, and/or hosted and non-cloud

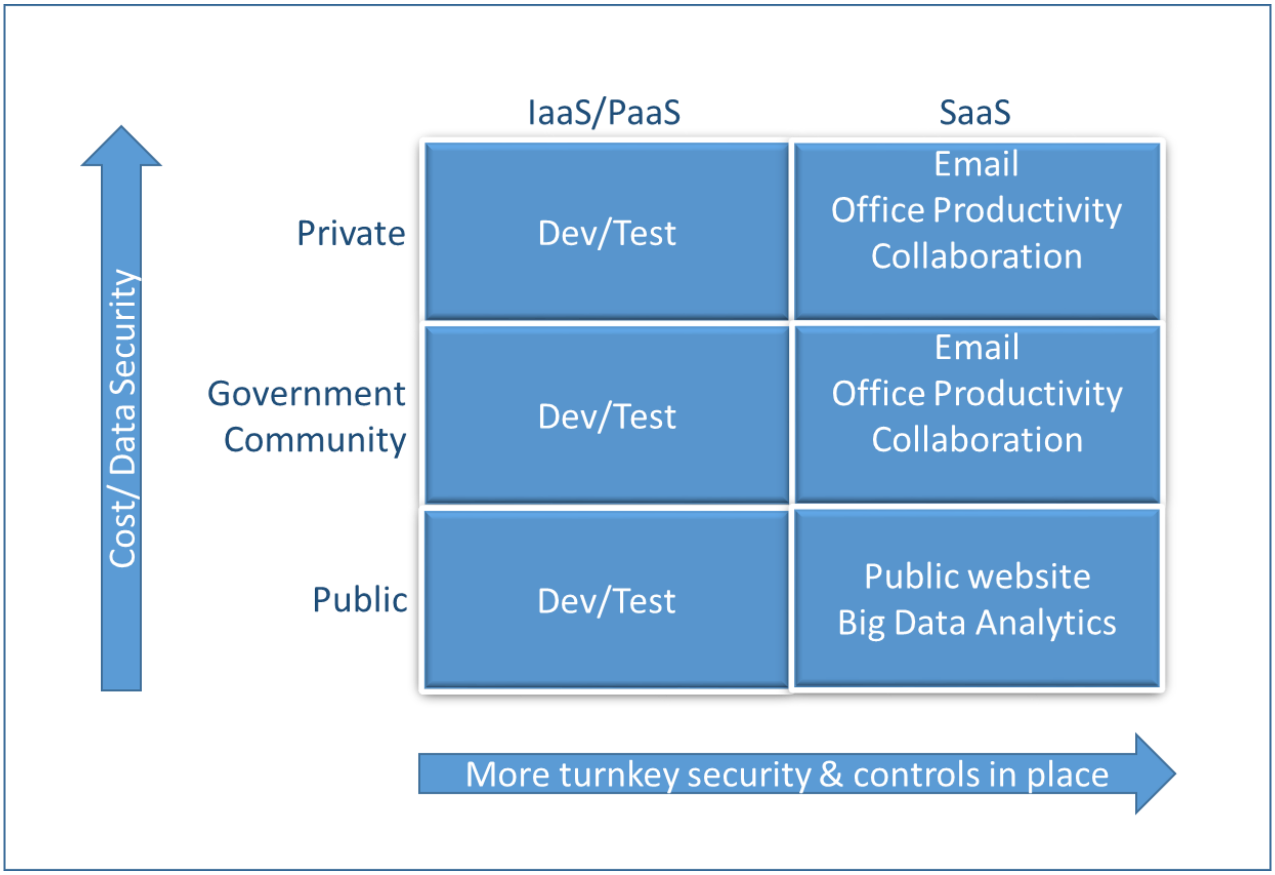
Several barriers to cloud adoption were discussed:

- **Policy:** Data protection and compliance, interoperability and data portability, identity and access management, auditing, adaptability, and availability are areas of concern.
- **Funding:** Agencies have neither the appropriate funding to migrate existing applications nor the appropriate methods to establish budgets for a fluctuating costs.
- **Long term viability of Cloud Service Providers:** Agencies are concerned about losing access to their data should the cloud service provide (CSP) go out of business.

[1] NIST, The NIST Definition of Cloud Computing, Special Publication 800-145.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- **Operational Changes:** Agencies require fewer internal IT personnel in the areas of infrastructure management, technology deployment, and maintenance. Therefore, operational changes will be required in areas such as disaster recovery, continuity of operations, monitoring, and oversight.
- **Lacking cloud knowledge and expertise**: Agencies typically have neither the necessary tools nor staff to implement cloud services.
- **Ensuring data portability and interoperability**: To preserve their ability to change vendors in the future, agencies may attempt to avoid platforms or technologies that "lock" customers into a particular cloud.
- **Overcoming cultural barriers**: Agency culture may act as an obstacle to implementing cloud services.
- **Procuring services on a consumption (on-demand) basis:** Because of the on-demand and elastic nature of cloud services, it can be difficult to define specific quantities and costs of consumption. These uncertainties make contracting and budgeting difficult due to the fluctuating costs associated with elastic and incremental cloud service procurements.

Finally, the discussion concentrated on where and how agencies are currently utilizing cloud services. The figure below depicts that as transitions from public, government community, and private deployment models in which the cost increases as well as security of data. Similarly, as one transitions from IaaS, PaaS, SaaS service models there are more controls and standard security in place.



|  | IaaS/PaaS | SaaS |
|---|---|---|
| Private | Dev/Test | Email<br>Office Productivity<br>Collaboration |
| Government Community | Dev/Test | Email<br>Office Productivity<br>Collaboration |
| Public | Dev/Test | Public website<br>Big Data Analytics |

Recommendations:

- Identify opportunities for procurement of cloud services on a consumption basis
- Establish cloud brokers or champions within agencies adopting cloud technologies
- Collaborate with other agencies
- Use least restrictive deployment models to facilitate adoption
- Be part of the cultural change
- Create cloud computing education opportunities for IT and non-IT personnel

*The Umbrella of Acquisition*

The Umbrella of Acquisition session was intended to explore the challenges of adopting cloud computing in the government due to contractual, cultural, and budgetary constraints. The goal of the session was to outline recommendations for constructing contracts to ease adoption of cloud computing, establish best practices for cloud adoption, and coming up with a common method of calculating the return on investment of cloud computing adoption.

The goals of this session included:

- Identify contracting vehicles that ease the challenges of cloud adoption
- Discussing best practices for cloud contracting and adoption
- Discuss common methods of defining the return on investment for cloud adoption

This session identified the following needs:

- The government needs to establish a revolving fund which can cover incurred pay-per-use charges, especially across fiscal year boundaries
- The government, industry, and academia need to establish open standards for interoperability between CSPs
- The government needs to consider making changes to the Federal Acquisition Regulation (FAR) to include provisions for commodity cloud services as utilities
    - The NIST definition of pay-per-use needs revisiting
- An organization should craft standard contracting language that can be used by multiple government organizations as a template
    - Language should include best practices that other agencies have identified and proven through lesson learned (e.g., handling data destruction, retention, or handling regulations)
- Government agencies that are moving to the cloud need to get business processes in order first so that they take advantage of cloud’s benefits

The summary of the collaboration session is below:

The Umbrella of Acquisition session discussions started with four topical questions posed by the session leads. First, from the perspective of a CSP, how effective has the government been in developing clear, specific scopes of work that enable the effective development of solutions for the government's requirements? Second, the cloud PMO most often deals with agency CIO staff in developing requirements and selecting acquisition vehicles but it is the CO staff that executes the procurement. The CO staff is less familiar with cloud technology; how do we reconcile disconnects between both groups of customers? Third, GSA is striving to be as consistent as possible when providing cloud vehicles. Can GSA modify or change how it buys and sells cloud services to be more consistent with private industry within the limitations of the FAR? Fourth and last, despite the government's "Cloud First" policy, cloud migrations are not occurring as fast as many people would prefer. What are today's known federal acquisition process limitations and challenges that inhibit cloud adoption across the government? What steps have been taken to address these challenges in recent years?

The discussions in the session identified several key outcomes. A recurring topic at the summit was vendor lock in and cloud exit strategies. Vendor lock in remains one of the biggest risks in the cloud. It is easy to get into the cloud but moving workloads and data out of a CSP is a technical and legal challenge. A transition plan (exit strategy) needs to be defined up-front and agreed to by all parties to avoid vendor lock in and close out at the end of a period of performance.

Price transparency from CSPs and matching price with the needs of the customer is important. There currently is no standard model for pricing services (per unit cost) across CSPs and can be very dynamic, making a standard GSA schedule difficult to maintain and comparing value of services difficult to compare. Other costs need to be considered in contracts such as cleanup costs and accountability resulting from a data breach.

With multiple government organizations pursuing cloud solutions, costs could be significantly reduced with overarching contractual agreements. If the government can aggregate contracts with CSPs across multiple agencies, the end goal could result in a negotiated discount based on volume. Sub contracts will need to be homogenized into standard contracts specific to the end-user or end-consumer. For example, if a government or contractor representative creates a virtual machine in a government cloud account, they technically could be obligating the government if the pricing is based on on-demand usage.

Finally, the discussion concluded that the cloud should be treated in the same way as other utilities (e.g., phone, electricity) with variable consumption. Rules may be different based on use of a CSP's public cloud, private cloud, or hybrid cloud classification, but the product should be treated as a utility.

Top Discussion Points:

- Vendor lock in and an appropriate exit strategy remain top challenges
    - Price transparency and comparable unit costs need to be improved to help measure return on investment
- Overarching government contracts could reduce cost by purchasing in bulk
- Cloud should be treated as a utility rather than a commodity

*Tiered Architectures*

The Tiered Architectures session was intended to generate a discussion around the movement toward tiered architectures and the impact of security zones, common hardware, and cloud integrity. The goal of the session was to discuss challenges facing the adoption of cloud with respect to identity access management (IdAM), ensuring operational and data integrity in public clouds, and exploring the feasibility of shared environments.

The goals of this session included:

- Explore cloud IdAM
- Discuss best practices and feasibility of adopting shared environments with multiple classification levels
- Identify barriers of adoption of tiered approaches, including technical challenges

This session identified the following needs:

- Improved contractual agreements
- Shared Request for Proposal (RFP) templates
- To strengthen trust in relationships between government cloud consumers and cloud providers:
    - Need to establish cyber incident reporting procedures and detection agreements
    - Change management and software platforms should change at each level
    - FedRAMP contract clause should be expanded
    - Best practice should be established for information sharing
- Continuity of Operations (COOP)/Disaster Recovery Plan
    - Continental United States (CONUS) and clearance is required for access and management
- Use FedRAMP as a baseline for requirements with many levels of goodness for the respective tiers
- Service providers should have a better understanding of the business requirements to provide better service

The summary of the collaboration session is below:

The session started with the discussion topics posted by the session leads. The topics include: How can multiple security classifications (e.g., TS vs. FOUO) exist on the same hardware? What policies must be in place to enable this heterogeneous environment? How can the government incentivize cloud providers to protect government data? How can FedRAMP expand or be improved to handle multiple user or security classifications?

The session identified the current challenges with the major challenges focused on security, geography, and operational concerns. In the area of security, the session discussed issues dealing with:

- Different classifications systems on the same platforms

- Challenges on how to separate classified systems or national security level systems verses non-national security level systems
- Federal Information System Management Act (FISMA) High (FIPS 199 High)

Ideally, lowering the sensitive data is preferred to enable cloud adoption. Different challenges exist within the adoption landscape, such as co-mingling national security systems with non-classified systems versus non-national security systems and non-classified systems. Finally, IdAM remains a challenge, particularly in shared environments.

The session continued the discussion on cost versus risk management, templates for various workloads, and related questions such as: Can workloads be compartmentalized? Is a boundary a suitability fit regarding the separation of mission applications within the cloud environment? These challenges impact a variety of aspects in the cloud industry such as:

- COTS solutions
- Guaranteed security
- Permissions that follow data
- Classification of data
- Sophistication of threats
- All about the data, things to consider cost vs Risk
- Identity and access control
- Encryption at storage level
- PIV/CAC/Credentials
- Middleware
- HIPAA
- Attestation
- Inter-Agency Sharing
- Service Level Agreement (SLA)
- OpEx vs. CapEx Cloud
- Data Loss
- Compromise (Federal vs. State)
    - Separation between Chief Information Security Office and Chief Information Officer
- Storage Service Provider (SSP) controls vs SLA
- Multiple levels on the same resources
- Geography
- Security personnel
- Features of a cloud's physical location:
    - Performance
    - Bandwidth
    - Latency
    - Optimized virtual desktop infrastructure (VDI) solutions
    - End to end protection

    - Network Operations Center, backup, support in different locations
    - Supply Chain/Equipment Integrity
    - Data Encryption
    - Key Management System/Key Escrow
    - Noisy neighbors
    - Over-subscription
    - Guaranteed
    - IOPS (Input/Output operations per second)
    - Trusted Internet Connection (TIC) not cloud-friendly
- Geography
    - Flood Zone Disaster Recovery
    - Hybrid solutions
    - Load Balancing
- Operational Concerns
    - Application Upgrades/ Operating system changes/patches
    - Change of Management
    - Control over supply chain
    - Portioning, based on customer requirements
    - Backups
    - Cyber Defense
        - Reporting
        - Additional monitoring
        - Incident Reporting
- Financial stability of CSP
- Data Rights

Finally, the session concluded that many of these concerns can be mitigated through improved contractual agreements. A good contract agreement can solve or prevent many of these issues. Improved contracting vehicles can lead to better support from cloud providers and such vehicles should be established using common templates for the greatest interoperability and sharing within the government.

The session identified the following needs:

- Put all business needs in the contract, including:
    - Data rights and data ownership
    - Backups, disk requirements, and disposal procedures
    - Application access rights and monitoring, even though it is not common but recommended
    - Put technical requirements inside contract
    - Aids in the consistency of having multiple agencies use the same infrastructure
- Shared RFP Templates
- Trusted Relationships:

    - Need establish cyber incident reporting procedures and detection agreements
    - Change Management and software platforms should change at each level
    - FedRAMP contract clause being expanded
    - Establish best practice for information sharing
- COOP/Disaster Recovery Plan
    - CONUS and Clearance is required
- Visibility
    - How broad is the scope of current vulnerabilities

*The Role of Cloud Computing Emerging Technologies*

The Role of Cloud Computing Emerging Technologies session was intended to explore the relationships between cloud computing and other emerging technologies, including mobile, big data, and the Internet of Things (IoT). The goal of the session was to discuss how these emerging technologies enabled one another, are inter-related, and can be adopted in tandem to realize larger, more impactful benefits.

The goals of this session included:

- Discuss how cloud can aid the adoption of mobile, IoT, and big data
- Discuss how cloud and other emerging technologies impact one another
- Identify ways in which cloud is expected to provide future benefits to emerging technologies and the government

This session identified the following needs:

- Characteristics and environments unique to emerging technologies in government need to be identified or developed
- Appropriate access to enabling emerging technologies needs to be provided
- Policy and training to enable adoption of emerging technologies needs to be created
- Cost of adoption vs. non-adoption of emerging technologies needs to be evaluated
- Quantifiable metrics (e.g., time value of money, time to use, cost of use, risk assessment) for emerging technologies need to established
- Ability to leverage emerging technologies that requires cloud computing needs to be recognized

The summary of the collaboration session is below:

The Role of Cloud Computing Emerging Technologies session discussions identified several challenges which need to be considered. A primary topic discussed was when and how to use cloud computing to enable the adoption and consumption of emerging technologies, and the need for work towards better definitions, revised policy, improved training, and improved risk assessment. Emerging technologies are more mature than cloud computing. Paired with the government adoption challenges and low consumption rate in industry, it reduces the likelihood that cloud computing is a strong enabler of emerging technologies. Government applications are not sufficiently optimized for the cloud, and therefore will not yet drive wide-spread adoption of emerging technologies in the cloud. However, to improve the likelihood of cloud enabled emerging technologies, use cases and justified use should be defined, along with enumerated pros and cons of using cloud computing.

As with other collaboration sessions, the cloud acquisition process was identified by this session as an area of concern. Specifically, the emerging technologies adoption and acquisition time frames and processes do not match the cloud acquisition process (e.g., the cloud acquisition process is not dynamic enough to be relied on by emerging technology implementers). Value measurement, defining return on investment, and making value propositions are current challenges with emerging technologies.

Liability cost was identified as an area in need of improvement to ensure security breaches are handled by the accountable party. Cloud security is still an area of concern within the government, particularly with respect to access, IdAM, and authentication. Similarly, the geographic location and integrity of the data being stored in the cloud remains a concern. In order for cloud to enable emerging technologies, the consumers of the cloud-hosted data must have an established trust of the data consumed from and stored in the cloud. Additionally, end-to-end solutions and models must be constructed to establish use cases and operational models for emerging technology adoption.

Standard cloud infrastructures and models (i.e., hybrid, private, public, etc.) are still loosely defined. Improving these definitions and standards would more easily enable the interoperability of clouds as well as improve the interoperability that is required when working with emerging technologies. For example, IoT is expected to have many end-points, and interoperability in a heterogeneous environment will be required to enable cloud and IoT integration.

Emerging technology implementers should understand that Internet access is assumed but not always available. The Internet is not ubiquitous enough to enable emerging technology use cases (e.g., census collection, critical infrastructure data collection).

The following emerging technologies were identified and use as a basis for framing the rest of the discussion and resulting recommendations:

- IoT
- Mobility
- Big Data
- Wearables (part of the larger IoT)
- Social Networking
- Containers such as Docker[2]
- Application Streaming
- Software Defined Networks (SDN)

While Big Data may be an exception within government agencies, other emerging technologies do not have a strong value proposition for adoption in the cloud. Cloud computing enables and is helping drive

[2] https://www.docker.com/

the adoption of big data practices. The Freedom of Information Act (FOIA) is a use case that spurs the adoption of Big Data analytics. There is also an increased demand for immediate, real-time data analytics to solve problems, make decisions, and meet mission goals. Quick set-up tools such as Docker will increase demand for Big Data solutions as these tools are adopted.

OLAP (On-line Analytical Processing) and OLTP (On-line Transaction Processing) systems leverage Big Data to enable real time decisions. OLTP emphasizes for OLTP systems is placed on very fast query processing, maintaining data integrity in multi-access environments. OLAP is characterized by relatively low volume of transactions. Queries are often very complex and involve aggregations. OLAP applications are widely used by data mining techniques which provide views of various kinds of business processes within an agency.

Cloud scalability will enable agencies to deal with storing, accessing and leveraging vast amounts of data that are needed to carry out many agency missions; the accessibility of data in the cloud will enable adoption of Big Data. In order to leverage accessibility as an enabler, agencies will need to convert legacy data sources into electronic, digital, or automated data sources. Data inconsistencies need to be addressed to enhance searching for relevant, mission focused data. This includes the consistency of data formatting to enable agencies to leverage data warehousing.

Cloud computing aids emerging technology adoption in the following ways:

Mobile and Bring Your Own Device (BYOD) adoption:

- Flexibility
- Accessibility
- Security Posture
- Cost Savings
- Connectivity
- Communication – in disconnected mode
- Does not equate to convenience or efficiency

Cloud Computing Aids IoT Adoption:

- Filtering capabilities
- Elasticity – manage types of data and connected edge devices
- Use smart technologies to create intelligence by “learning” data needs

Recommendations:

- Identify characteristics unique to emerging technologies
- Provide appropriate access to emerging technologies to facilitate and encourage experimentation
- Policy and training investments need to be improved
- Recognize the cost of not adopting the cloud

- Quantify the value added with respect to risk assessment, time, and money investment
- Emerging technologies require the cloud to be successful and ubiquitous at all levels

Cloud will not solve or address all emerging technology issues. Use cases or challenges such as connectivity or high cost processing for applications cannot be solved by a cloud implementation. Defining how cloud computing is value added to emerging technologies will speed adoption.

## Summit Recommendations

Each collaboration session produced common themes. Many of the challenges identified at past summits have been addressed in part, but the same challenges still exist. For example, FedRAMP is now widely accepted as a good, established baseline for minimum cloud security implementation. While acquisition remains a key challenge, success stories are beginning to appear, and best practices and recommendations are emerging. One of these recommendations is to include exit strategies in the contracts to ensure data can be pulled from a cloud provider at the end of a period of performance. While these challenges persist, they are being mitigated by government practitioners.

Other challenges and common themes came out of the collaboration sessions. The participants recognized that financial savings is becoming secondary to the performance and long-term benefits of adopting emerging technologies, including cloud computing. Cloud computing is becoming the enabler of other emerging technologies, as well. Lacking from the cloud computing domain are metrics to assess adoption effectiveness, true cost of adoption (e.g., benefits of automation), cost of delaying adoption (e.g., reduced capabilities or higher costs later in the lifecycle), and a standard unit of cost.

The government does not have a standard method to identify which cloud provider or even type of cloud would be most beneficial for adoption. To mitigate this – and other – risk and challenge, agile processes should be used when adopting cloud computing; this includes continual engagement, small but frequent deliverables, and fail-early models.

The summit participants also identified FedRAMP as a “good start” to cloud security. The participants recognized FedRAMP as an accepted standard that identifies the minimum set of security that needs to be in place for cloud adoption. Several participants identified the need for finer grained – or customized – controls to be put into place to help tailor the set of standards to particular organizations, cloud providers, and project goals.

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 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.

## Conclusion

The January 2015 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 challenges, acquisition barriers, and technical understanding remain difficulties to overcome. The adoption of agile processes, increased collaboration, and improved education and training can help mitigate the identified challenges.

While the January 2015 Federal Cloud Computing Summit highlighted areas of continued challenges and barriers to adoption (e.g., agency culture, budgeting mismatches), the Summit also cited notable advances in mitigating these perennial challenges. For example, budgeting models that include spending and usage rate controls and caps have been noted as suitable mitigations to fixed-budget models for elastically consumed services. Similarly, cloud computing is largely accepted as a desired end-point, but wider cultural opinions are shifting to an understanding that cloud computing should be adopted for suitable solutions. In short, the community has made advances toward overcoming the challenges historically associated with government cloud adoption, but work still remains to be done before these challenges are entirely mitigated.

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.

**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 author.**

**Approved for Public Release; Distribution Unlimited. Case Number 15-1080**