CLOUD COMPUTING:

Risks, Benefits, and Mission Enhancement for the Intelligence Community

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

CLOUD COMPUTING TASK FORCE

MARCH 2012

ACKNOWLEDGEMENTS

INSA CHAIRWOMAN

Frances Fragos Townsend

INSA CYBER COUNCIL CHAIR

Terry Roberts, *Executive Director, Interagency Acquisition and Cyber, Carnegie Mellon SEI*

INSA STAFF

Ellen McCarthy, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Jay Fox, *INSA Research Fellow*

Aviva Cohen, *INSA Research Intern*

Joe Welty, *INSA Research Intern*

TASK FORCE WRITING TEAM

Bob Gourley, *Crucial Point LLC (Task Force Chair)*

Kevin Jackson, *General Manager of Cloud Services, NJVC, LLC*

Maureen McGovern, *President, KSB Solutions*

INDUSTRY TEAM

John Totah, *Oracle National Security Group (Task Force Team Leader)*

Steve Cooper, *Chief Information Officer, Federal Aviation Administration*

Ty Fabling, *Enterprise Systems Architect, ESRI*

Bill Gravell, *President, Diogenes Group, LLC*

John Howie, *Senior Director, Microsoft Global Foundation Services*

Dick O'Leary, *Global Director for Physical Security Solutions, EMC Corporation*

Nate Rushfinn, *Certified Enterprise Architect, CA Technologies Public Sector*

Dick Schaeffer, *Consultant, Riverbank Associates, LLC*

Mark Schultz, *Federal Intel Sales Manager, ESRI*

Michael Young, *Senior Enterprise Security Architect, ESRI*

GOVERNMENT TEAM

Maureen McGovern, *President, KSB Solutions (Task Force Team Leader)*

David J. Bishop, *Chief Technology Officer, LGS Innovations*

Gus Bontzos, *Vice President and Business Unit Director, ITT*

Nick Buck, *President and CEO at Buck Consulting Group, LLC*

Howard Clifford, *Distinguished Technologist, Hewlett-Packard Co*

Kevin Considine, *Partner, Federal Consulting Practice at CSC*

S. Gulu Gambhir, *Senior Vice President and Chief Technology Officer, Intelligence, Surveillance and Reconnaissance Group at SAIC*

Willis A. Janssen, *Director of National Security and Intelligence Programs, The Boeing Company Information Systems Group*

Dr. Martha Menard, PhD, *CMT Principal, Sigma Applied Research*

Mary Merritt, *Cyber Security Awareness and Outreach Compliance and Policy Section Cyber Security and Information Assurance Division*

Rick Parkington, *Vice President and Chief Technology Officer, General Dynamics Information Technology Intelligence Solutions Division*

Annette Redmond, *Enterprise Intel Operations, Department of Defense*

Samuel Visner, *Vice President and Cyber Lead Executive, CSC*

Teresa A. Weipert, *Senior Executive, Accenture Health and Public Service Technology Services*

Participation in the Task Force does not imply personal or official endorsement of the views in this paper by either the Task Force member or his/her office.

EDITORIAL REVIEW

Joe Mazzafro, *Captain USN (ret.), CSC Defense Intelligence Division*

COPY EDITOR

Elizabeth Finan

EXECUTIVE SUMMARY

In response to recent trends in federal information management to move towards cloud computing, the Intelligence and National Security Alliance (INSA) convened a working group to study the mission impacts of cloud computing on the Intelligence Community (IC). The Cloud Computing Task Force collected and analyzed data through a concerted effort in which two groups conducted over fifty interviews with thought leaders and policy makers in the public and private sectors.

Cloud computing provides information technology (IT) capacity in elastic ways that can expand to meet user needs and shrink when demand decreases. It enables far more agility in support of operational missions and expands access to computational power while potentially reducing operations and sustainment costs. Throughout our analysis, we found that in their adoption of cloud computing, organizations had to take responsibility of new roles and functions and revise their policies and processes. Cloud computing's primary value does not lie in being a new technology; instead, it represents a business model change whose rapid adoption is driven by the transformative nature of its integration.

Within the IC, cloud computing uniquely addresses critical defense and intelligence mission needs by locating data and applying it to the mission at hand. As a bonus, cloud computing offers DoD and IC agencies the ability to increase efficiencies and potentially realize cost savings during their lifecycles to alleviate some of the pressure of budget reductions. Still, there is a significant gap in understanding cloud computing at all levels, which could impact the success of a cloud solution deployment.

The most fundamental change that needs to occur is in the organizational cultures of the IC. While in the past federal funding has been allocated based on what information and capabilities an organization controlled, there is a vital need to change this mindset to encourage information sharing across the IC. In order to take full advantage of a cloud model, it will also be necessary to update the Federal Acquisition Regulation.

If successfully implemented and managed, cloud computing approaches and technologies can transform the Intelligence Community's computing capabilities by more efficiently and effectively enabling the majority of IC functions. As cloud computing innovations are adopted, we expect to see improvements in security and IT efficiency, but only if end-to-end requirements, designs, and architectures are carefully considered. The IC must pilot new ways of partnering across government, academia, and industry to ensure continuous and productive cooperation.

Based on information collected from nearly 50 interviews, the Cloud Computing Task Force drew the following conclusions:

1. Decision makers in the IC are appropriately focusing on the business model implications of cloud computing. Cloud computing is not just a new technology, but a significant shift in the consumption of IT resources and allocation of IT funding.

2. Within the IC, the decision to adopt a cloud model is focused on mission enablement and must be determined on a case-by-case basis. The evaluation of cost savings must bear in mind costs over the complete lifecycle, rather than a periodic budget cycle.

3. Information security can be enhanced through a cloud computing approach, but only when it is built into the model's design. If security is not part of the design, cloud computing architectures dramatically increase risk.

4. The type of cloud deployment model adopted will be determined by the sensitivity of data hosted.

5. Those looking to migrate to the cloud must consider impacts on organizational culture.

6. Improvements to how agencies acquire services, software, and hardware are strongly desired by most personnel involved in the implementation of cloud computing, and many believe that the adoption of a cloud solution may catalyze these changes.

7. As standards for cloud computing emerge, thoughtful federal input can contribute to greater security and cost efficiencies. Any organization contemplating adopting a cloud architecture, including those within the IC, should include the ability to support multiple standards.

8. Lessons learned from the IT industry, the private sector, and academia must inform IC decision making. Sharing lessons learned is essential to reducing risk.

I. INTRODUCTION

On August 24, 2006, Amazon turned on a new capability called the Elastic Compute Cloud (EC2). This offering of inexpensive, on-demand computing power ushered in a new era of rapidly changing business strategies, technologies, and functionalities. A business gamble that pundits called "Jeff Bezos' Risky Bet"[1] ended up changing an industry and dramatically impacting the national security field. Indeed, cloud computing is a topic of significant interest to the intelligence and defense communities because of its potential to deliver more IT capacity at a lower cost.

> Cloud computing represents a business model change that has already had a significant impact on the intelligence mission.

The purpose of this paper is to provide actionable information to the IC, including government and industry decision makers who are wrestling with the best ways to gain the benefits of cloud computing. The IC has important mission needs and security requirements that must be taken into account when considering cloud computing approaches. This paper articulates many of these needs. The community also shares efficiency goals with other parts of the federal enterprise, and insights into the issue of cost savings are provided here. This paper includes input from thought leaders in cloud computing communities in government, industry, and academia. These thought leaders are driving innovation in hardware, software, and business models that are directly applicable to national security architectures. Through interviews and research, we provide results that should further the discussion among senior decision makers on the future of cloud computing in the federal government. We focus on the two most predominate forms of cloud solutions: clouds for utility computing (like those described in the National Institute of Standards and Technology [NIST] Definition of Cloud Computing) and data-intensive clouds (such as those fielded to run the analytics of Google, Facebook, Twitter, LinkedIn, and USA.gov searches).

Many agencies have a wealth of experience in cloud computing approaches, and we believe their lessons learned will be relevant to others in the federal space who are adopting cloud optimization strategies. Director of National Intelligence (DNI) James R. Clapper has brought cloud computing into the lexicon of senior mission executives in hopes of enabling consolidation and continued mission support in periods of significant budget pressure. Changes to cloud approaches are on the horizon, making this a good time to reexamine the thoughts of experienced community professionals on this topic.

METHODOLOGY

In order to study the mission impacts of cloud computing on issues relevant to the IC, INSA convened the Cloud Computing Task Force. INSA's members have extensive experience in national security operations and issues, and constitute a unique cross-section of government, industry, and academia. Our unique position along the public-private divide enables us to inform government decision making in ways that internal sources of information cannot, providing exogenous thought that sheds light on the IC's mission needs. We also seek to inform the private sector of the cloud solution needs of the IC.

To this end, the INSA Cloud Computing Task Force researched emerging cloud technologies and interviewed a wide spectrum of government and private sector decision makers to produce a report with insights relevant to senior policy makers, IT professionals, and the acquisition cadre in the IC. We also established a means for continuing research and dialogue, and invite your comments on this document to further the body of knowledge around the national security implications of cloud computing.

The Cloud Computing Task Force collected, consolidated, and analyzed data through a concerted effort in which two groups (industry and government) conducted over fifty interviews with thought leaders and policy makers in the public and private sectors. Interviews with the public sector sought to highlight current adoption plans, identify key drivers, and appreciate technological and organizational barriers to adoption. The organizations targeted are associated with the Department of Defense (DoD) and the IC—agencies with unique security and mission needs. The private sector interviews were geared towards understanding industry cloud adoption models and recommendations, as well as trends in emerging cloud technologies. The data analysis consisted of drawing out common themes brought up by both federal and private sector participants in order to frame a general discussion of the government's needs and guidance from the private sector.

DEFINITIONS

Decision makers in the IC use the term "cloud" in one of two ways: as an adjective or a noun. As an adjective, it refers to a method of computing. As a noun, it refers to an emerging IT infrastructure that supports these new business processes. Both uses of the phrase "cloud computing" are used in the rest of this document. We recommend others make this distinction as well to help remove ambiguity.

Cloud Computing as an adjective: A method of computing that provides IT capacity in elastic ways to expand to meet user needs and contract when demand decreases.

Cloud Computing as a noun: An infrastructure of on-demand capabilities using virtualized resources. This involves pools of storage, network, processing, and other computational resources that can be efficiently allocated when requested and quickly provisioned in a highly automated fashion.

The NIST Special Publication 800-145, "The NIST Definition of Cloud Computing," defines relevant terms as well as the deployment and service models for cloud computing. For the sake of consistency, we have used the following NIST definitions of cloud computing.

Five characteristics of cloud computing:

1. On-demand self-service
2. Ubiquitous network access
3. Location independent resource pooling
4. Rapid elasticity
5. Measured service with pay-per-use

The cloud computing deployment models are:

Public Cloud
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Private Cloud
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud
The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.

Hybrid Cloud
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting[2] for load balancing between clouds).

The cloud computing service models are:

Software-as-a-Service (SaaS)
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform-as-a-Service (PaaS)
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Infrastructure-as-a-Service (IaaS)
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems: storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

SaaS
Consume

PaaS
Build

IaaS
Host

II. RECURRING THEMES

CLOUD COMPUTING IS A BUSINESS MODEL

We found that leaders in government and industry primarily view the benefits of a cloud computing architecture to be a result of the business model changes required by its implementation. Cloud computing represents a business model change whose rapid adoption is driven by the transformative nature of its integration. We found that the successful adoption of a cloud model would necessitate significant changes not only in IT strategy but also in agencies' acquisition processes, workforce, and culture, and we underscore these points later in our review. This position diverges from the Government Accountability Office's stance that "cloud computing is a new form of delivering IT services that takes advantage of several broad evolutionary trends in information technology, including the use of virtualization"[3] by emphasizing cloud computing's impact on the federal business model and organizational culture. As highlighted by one IC official, "Keep in mind that cloud is never 'done.' It is a way of doing business, an approach, not a 'thing'."

Cloud computing represents a business model change whose rapid adoption is driven by the transformative nature of its integration.

According to Jim Cooke, Senior Director of Cisco's IT Transformation Practice, "Technology is not the primary impetus to shift from traditional, data-center-based IT, and the technologies that underpin cloud computing are not new. Rather than experiencing a technological revolution, we are seeing a change in the way we consume IT resources. The shift is due to the economics of using the cloud computing model versus the physical data center."[4] Dramatic increases in network and processing speeds have lowered the cost of one megabyte of storage from $70,000 to about a tenth of a cent, making the cost of storage 10 million times less expensive.[5] Advances in virtualization technology and the realization among Chief Information Officers (CIO) that non-sensitive data and processes can be hosted with a third party vendor have been important aspects in the rise of cloud computing. This business model is defined by flexibility and rapid scalability. It was apparent to us that decision makers in the IC are appropriately focusing on the business model implications of cloud computing.

Many agencies echoed one IC technical executive's belief that "cost savings are expected but not yet understood," and saw a need for comprehensive cost analysis prior to adoption. However, some organizations have seen marked cost reductions as a result of cloud adoption; for example, one agency saw a directorate minimize hardware costs by 40 percent (largely due to consolidation enabled by the cloud approach). Such decreases in hardware investment are expected throughout the community, and are one step in a cloud deployment. Under the Federal Data Center Consolidation Initiative (FDCCI), the government plans to close 800 of more than 2,000 federal data centers by 2015, saving over $3 billion annually.[6] Many agencies have stated that

cloud adoption is essential to gain cost efficiencies and maintain performance in the face of upcoming budget cuts. However, it may be useful to frame our discussion of cloud computing in terms of how cloud computing enables cost avoidance. In cloud deployment models, costs will shift from hardware and software management/upgrades to fixed spending on vendor management and Service Level Agreements (SLA). This does not inherently suggest a reduction in IT spending. However, cloud computing promises far greater transparency in managing operational costs, which may decrease "unexpected" costs.

A 2011 study by CSC showed that more than half of organizations surveyed saved little or no money after transitioning to cloud computing.[7] Only 14 percent of organizations surveyed actually downsized their IT departments after moving to cloud architectures. Enthusiasm to adopt a cloud solution must be tempered by the fact that the economic value of cloud computing can only be realized when the necessary scale and customer set diversification is also present. Agencies expecting immediate cost savings simply because they have adopted a cloud model will be greatly disappointed if the economic model is not also appropriately designed, modeled, implemented, and monitored. One CIO believes that the biggest "bang for your buck" will probably come from interoperability that cloud computing enables "up the stack" (from software to the data and application layers). It was suggested by one federal Chief Technology Officer (CTO) that cloud implementations may cost more in the short run (especially for private cloud models), but will provide significant mission value. The impact of cloud computing on the mission was repeatedly emphasized and ranked far higher than economic benefit as a driver for government adoption. The main drivers included mission success, cost avoidance, data analytics, information sharing, and access to innovation.

Government agencies that have just moved to the cloud may find that their architectures are not truly optimized to take advantage of cloud technologies. This flows from incorrectly equating data center consolidation and virtualization to cloud computing. It may be efficient for agencies to geographically consolidate separate data centers into a single, larger data center, but this does not necessarily mean they are following a cloud computing approach. Canonical's Dustin Kirkland contends that "decision makers need to be aware that countless commercial offerings have simply been re-branded 'cloud' in marketing maneuvers designed to ride the waves of popularity associated with cloud computing." Decision makers need to separate the noise from the signal and ask, "Am I really dealing with the cloud, or a marketing message?"

Government agencies that have just moved to the cloud may find that their architectures are not truly optimized to take advantage of cloud technologies. This flows from incorrectly equating data center consolidation and virtualization to cloud computing.

CLOUD COMPUTING IS A KEY MISSION ENABLER

Across the IC, cloud computing is seen as a key mission enabler. From data analytics and information sharing to innovation and cost efficiencies, cloud's operational significance is extremely important. Lieutenant General Richard Zahner (U.S. Army, Deputy Chief of Staff, G-2) stated that the main drivers for the Army's cloud adoption are analytical capabilities set against intelligence problems characterized by massive data sets, as well as the potential for concurrent access to data by analysts at multiple echelons. Dr. Russell Richardson, Chief Cloud Architect at INSCOM, is adamant that some mission functions cannot be accomplished without cloud computing architectures. The significance of cloud computing to these missions is that it enables users who might otherwise be unable to afford, host, or operate large data centers to access shared and virtualized large-data processing capabilities.

From data analytics and information sharing to innovation and cost efficiencies, cloud computing's operational significance is extremely important.

Within the IC, information is often the decisive discriminator. Studies of recent mission failures found that many were caused by:

- The compartmentalization of information in data silos;
- Weaknesses of the human-based document exploitation process; and
- A reliance on "operationally proven" processes and filters typically used to address the lack of computational power or decision time.[8]

In most of these cases, the critical piece of information necessary for mission success was already possessed. The failure was not in obtaining the information but in locating and applying it to the mission. Cloud computing can address such issues, as well as enabling multi-use intelligence. Cloud solutions can now be used to work on all of the data, all of the time. With the ability to leverage the power of a supercomputer at will, critical decision timelines can now be more easily met.

Many of the mission contributions from data analytics flow from the emerging discipline of "Big Data." The amount of data being created is growing faster than humans can analyze. But fast analysis of this data is required to meet important mission needs. This is driving the continual pursuit of new solutions to Big Data challenges. The field is being led by programmers and computer scientists who handle overwhelming amounts of data from Internet-based capabilities, but have been generating many lessons and capabilities directly relevant to government mission needs. Cloudera CEO Mike Olson called this period in time a "Cambrian Explosion" of Big Data approaches and credited the open source software community and Apache Foundation for enabling the solutions the IC is fielding.

DECISION TO ADOPT MUST CONSIDER APPROPRIATE FIT

At GEOINT 2011, DNI Clapper stated that "Cloud computing is not a panacea," suggesting that the cloud does not solve all mission or technology challenges. The decision to adopt cloud technologies requires careful consideration and the development of a business case with total life cycle costs included. True cloud computing means elasticity, and that requires design. Simply moving applications to a cloud computing environment is not sufficient, so it is necessary to understand what it takes to rewrite true cloud-based applications. One example of a change in mindset that IT technicians must adjust to is moving business services (rather than technical components) to the cloud. The incorrect attitude is to move 1000 servers (that are supporting 10 business processes) to a cloud computing architecture; instead, the goal should be to move 10 different business processes to the cloud environment. Agencies need to consider business services and not just the IT components that support them.

Analysis must be conducted to determine if cloud computing is a good fit. For example, when an application uses an entire physical machine or is sized to use multiple dedicated physical machines, then it may not be a good candidate for moving to the cloud. Specialized applications that are not written explicitly for cloud architectures may be hard to migrate, as well as traditional enterprise systems where dedicated hardware is used for business or mission critical services.

Any application that needs detailed traceability at the user and device level may experience issues in a cloud environment. If there is not much elasticity required, the applications may run in the cloud, but they will not take advantage of cloud computing capabilities. An extremely stable environment where demand does not fluctuate and can be calculated may not need a cloud solution. It was suggested that mission-critical applications should not be moved, especially where lives are on the line (such as combat systems that direct the actions of soldiers in the field) until cost, benefit, and reliability are clear. To be useful, a move to the cloud must not only enhance mission effectiveness, but also make sense within the mission's context. Our conclusion from talking to both industry and IC practitioners is that the decision to adopt a cloud model needs to be focused on mission enablement and must be determined on a case-by-case basis. The evaluation of cost savings must include the entire lifecycle of the mission requirement.

SECURITY WILL REQUIRE INNOVATIVE THINKING

No two cloud solutions are alike, and it was generally agreed that each federal agency has a different perspective on the requirements and meaning of a secure cloud solution. In general, all cloud architectures that serve the government have a need for elevated security (such as the Federal Information Security Management Act Low/Moderate/High levels) and share some basic foundational elements.

Across the IC there is ambiguity on the use of the term "cloud computing." Research in the national security space has observed this before. For example, the Lockheed Martin Cyber Security Alliance report, *Awareness, Trust and Security to Shape Government Cloud Adoption,* states that "Knowledge is not necessarily widespread among agencies involved in cloud computing. Approximately one-fifth (21 percent) of respondents who are involved in cyber security at their agencies are not familiar with cloud computing, while nearly half (47 percent) of respondents who are familiar with cloud computing are not involved in cyber security."[9]

Rapid changes have also widened this gap. Neill Tipton, Director of Information Sharing and Partnership Engagement at the Office of the Under Secretary of Defense for Intelligence, believes that while many high-level members of the IC are knowledgeable on the state of cloud computing, "the necessary standards and processes to create timely intelligence based on data and services residing in disparate cloud implementations are not yet generally understood." Members of the IC echoed the lack of awareness at many levels in the community. This is especially troubling because the suitability of cloud computing adoption depends on a thorough understanding of the data and applications. These are best appreciated in terms of the traditional security triad of confidentiality, integrity, and availability; the security requirements of the organization considering the cloud deployment; the security capabilities of the cloud solution provider; and the risk tolerance of the organization.

The adoption of a cloud solution can provide security benefits, but only with planning and work. Without engineering focused on security, cloud computing can pose grave information security threats. However, moving to cloud-based solutions (whether deploying a public, community, private, or hybrid cloud model) can provide an opportunity to develop security protocols beyond "check the box" compliance. Still, awareness of security best practices and emerging threats is critical. The IC should address these important security aspects through the consistent operational implementation of cloud infrastructures across the following broad categories:

- Multi-tenancy: How can you ensure secure access to and separation of user-allocated cloud resources?
- Availability: How is data "up time" written into your Service Level Agreement?
- Confidentiality: How will your data be protected at rest and in motion?
- Integrity: How will you ensure that your data is not corrupted?
- Forensics: Can you monitor everything that has happened to your data and within your infrastructure?
- Data Location: Where is your data "living"?

In cloud models, there are many more management points (e.g., virtual machines) than in the traditional data center. New technical approaches tend to introduce new attack vectors, and there are new areas where specific controls need to be applied. Sophisticated detection systems are useful, but unfortunately the adversary may always be ahead of the curve that governs the response time for security breaches and events.

Do not expect the mitigation of information security risks to be inherently managed by cloud computing providers unless it is specifically written into your Service Level Agreement.

New risk management regimens that include identity and access management, change and configuration management, and the extension and introduction of new trust boundaries will also drive specific security controls for hypervisor layers, automation, orchestration, and the application programming interface. For a comprehensive cloud computing security model, fundamental Defense in Depth (DiD) best practices must be applied. DiD means applying controls at the physical, network, operating system, hypervisor, and application/user layer. In protecting cloud computing platforms, obvious technical controls (including virtual firewalls, encrypting disk images, and dedicated host servers) should be used. Agencies need to outline a data protection strategy and be aware of how cloud providers encrypt data both at rest and in flight and how their encryption keys are managed. The government should lead efforts to define key management infrastructure and encryption mechanisms as well as managing commercial vendors' roles in delivering encryption solutions based on clearly stated requirements. Access controls, authentication, and auditing (as well as end-to-end trust) must be established with cryptographically strong mechanisms. Identity and access controls must be enforced at both the network layer and the application/user layer in order to mediate the insider threat, which may be magnified in this environment. Rod Johnson, Senior Vice President of the Application Platform Division at VMware, comments that "in light of the Wikileaks disaster, there needs to be some kind of mediation layer that limits the amount of data that may be compromised by an insider."

Looking five years into the future, architectural best practices will be more established. The pitfalls of a cloud-based solution are the potential for massive amounts of data or day-to-day operations to be at risk of a zero day exploit (a software vulnerability for which there is no patch), potentially exposing or limiting the availability of that data. However, this is not a new danger. These pitfalls can be mitigated with careful planning, but the close proximity and commonality of the platform needs to be addressed by the security controls in place. Cloud computing is not a technology that implicitly or explicitly is "secure," "redundant," or "available," and using a cloud architecture is not a panacea relieving the requirements of sound system management. A number of outages in large cloud centers might have been mitigated with proper IT planning and the implementation of data replication practices, backups, and robust systems management. Cloud computing, with all of its advantages, does not negate the need to patch servers or choose a service provider with automated updates. As one private sector technology leader notes, "By moving to the cloud, you don't get waivers for information assurance controls and enforcement. There is no accountability as a service. You are still responsible." Do not expect the mitigation of information security risks to be inherently managed by cloud computing providers unless it is specifically written into your Service Level Agreement.

Cloud computing is not a technology that implicitly or explicitly is "secure," "redundant," or "available," and using a cloud architecture is not a panacea relieving the requirements of sound system management.

The view echoed throughout the interviews was that the IC must take an active role in cloud computing risk management. It is a fallacy to assume that cloud computing is less secure than a private data center that has access to the Internet. A key issue raised is that a very large percentage of breaches do not come from attacks on the cloud's architecture, but rather from insecure clients or third parties. "If you can't protect the client, you can't protect the cloud."[10] Third party trust is at once an essential part of cloud security and the most often overlooked. According to one business executive, "You need to be careful about who you pick as your partners." Establishing trust is essential and follows typical engagement processes and business practices. Security solutions are not just about identity management, traditional security, and secure applications, but also revolve around privacy and vendor trust. It is our conclusion that a cloud computing model derived from business goals must inherently build in elements for protecting the cyber domain using a risk management approach. Information security can be enhanced through a cloud computing approach, but only when it is built into the model's design.

THE LEVEL OF INFORMATION SENSITIVITY DETERMINES THE MOST APPROPRIATE DEPLOYMENT MODELS

As EJ Jones (Boeing Technical Fellow in Information Security) notes, it is widely accepted that "the level of information sensitivity determines the most appropriate model." Marwa Mabrouk, Managed Services Technical Lead at ESRI, explains that Certification and Accreditation requirements dictate cloud computing deployment and will most likely result in private cloud models being used for sensitive information.

There may be applications with characteristics or constraints that will not allow them to benefit enough from a cloud solution implementation to make adoption worthwhile; extreme classification requirements may be one such characteristic. However, at the low end of information sensitivity, there is a lot of unclassified information that requires processing, storage, and transmission that may be effectively managed with controls to quickly provision authorized access and with mechanisms to protect data integrity. In view of the information aggregation risk, public clouds may still be inappropriate for unclassified IC data. However, the use of unclassified government community clouds, such as the General Services Administration (GSA) IaaS Blanket Purchase Agreement (BPA), seems to be a useful public cloud proxy. Public-facing web sites (such as the .gov domain) may be optimally run on government community clouds using PaaS. For SaaS, workloads such as email, collaboration, and calendaring not requiring specialized sensitivity can go into a public or hosted private cloud. Victoria Kouyoumjian (IT Strategies Architect at ESRI) predicts that the hybrid model will be the optimal choice for the IC and may be described as a "private community-managed cloud."

Cloud adoption considerations include whether the program contains large amounts of public or unclassified information or can achieve cost reductions and increased performance from being hosted on a public cloud. It would be wise to leverage architectures with the potential to expand to a hybrid-private model when security considerations arise. As one CTO explained, "This must be looked at as an evolutionary model."

There may be applications with characteristics or constraints that will not allow them to benefit enough from a cloud solution implementation to make adoption worthwhile; extreme classification requirements may be one such characteristic.

One advantage of deploying a private or hybrid cloud is to get the benefits of cloud computing infrastructure for internal application purposes to comply with policy objectives. To understand how to begin moving towards such a cloud computing model, organizations must balance their internal policy and business objectives. Community clouds may evolve by taking existing adoption models and applying them to multiple DoD and IC agencies. The IC Common Operating Environment (a "cloud-like" project with NSA, NRO, NGA, DIA, and CIA participation) announced at GEOINT 2011 may develop into such an entity.

Cloud computing will have a major effect on the culture of the country's defense-industrial complex. The current norm is for prime integrators to oversee the entire product lifecycle, developing and operating "end-to-end" systems. In a cloud business model, the infrastructure and applications are separate accounts and programs. Today's resource-constrained environment will drive the IC towards a new set of solutions. The challenge will be for industry to meet this demand. One CEO suggested that the advantages of accelerating the use of commercially developed cloud models may be realized if the government "works with cloud providers and the Defense Industrial Base (DIB) to create some community-shared and agency-specific private clouds in secure but commercially owned and operated datacenters."

CLOUD COMPUTING WILL HAVE CONSIDERABLE IMPACTS ON ORGANIZATIONAL CULTURE

Throughout our analysis, we found that in their adoption of cloud computing, organizations had to both take responsibility of new roles and functions and revise their policies and processes. The most important duty organizations have when looking to adopt cloud infrastructure is to develop a better understanding of cloud computing in general, the associated security and IT issues, and how considerations of cost come into play. This is a tall order. Below the CIO and CTO levels across many of the federal agencies, there is still little appreciation for cloud computing's enabling capacity, and this stems from the overuse of buzzwords and the marketing of virtualized systems that are not necessarily in the cloud. The security of a cloud-based system is very dependent upon this understanding, as the adoption of cloud technology shifts the responsibility for information assurance to federal IT workers if vendors' responsibility is not explicitly written into the SLA. It will be impossible for federal agencies to secure systems hosted in a cloud environment without a thorough understanding of the architecture, vulnerabilities, and best practices beyond "check the box" compliance.

The most fundamental change that needs to occur is in terms of organizational culture. While in the past federal funding has been allocated based on what information and capabilities an organization controlled, there is a vital need to change this mindset to encourage information sharing across the IC. Because change is often viewed as a threat or risk to today's performance, this transition may not be easy. Jill Singer (NRO CIO) has seen that IC program managers and operators may exert a control and ownership mindset that extends to physical assets. The existing "control culture" may inhibit the use of operationally beneficial approaches such as allowing data to "live" at an agency, yet be accessed by others. Instead of emphasizing what individuals control, there needs to be a shift to focus on what managers enable, and organizations need to find a way to reward them for embracing and facilitating this change. Changing reward and incentive programs to encourage the "assist" may be necessary to develop a culture of information sharing. This shift highlights the importance of a focused cloud computing change management strategy.

One CIO noted that security in multi-tenant hosting facilities also remains a cultural concern and both the CIO security staff and the counter-intelligence staff play a key role in enabling the adoption of cloud computing in the IC. Agencies must ask themselves, "What is the impact on the people?" Those who have budgets and agendas to protect will resist change. Those who figure out how to capitalize on the cloud's capabilities have the best chance to succeed, and agencies who continue to use legacy models will face irrelevancy. The table below illustrates the organizational changes precipitated by the adoption of cloud technology.

Cultural Changes within the IC

Old Cultural Norm	New Cultural Norm	Manifestation Medium
Infrastructure-centric	Data-Centric	Security, Organizational Policy
Enterprise-Driven	More User-Driven	IT Infrastructure Design, SLAs, IT Standards
Purchase Tangibles (such as IT hardware)	Purchase Intangibles (such as virtual storage and processing power)	IT Procurement & Acquisition, Organizational Policy
Manage Tangibles	Manage Intangibles	IT Operations, Organizational Policy
Tightly Bound Physical Environment	Loosely Coupled Virtual Environment	Security, IT Infrastructure Design, Organizational Policy
Avoid Risk	Manage Risk	Security, Organizational Policy, IT Operations
Limited Resources	Infinite Resource Illusion	Resource Management, IT Procurement & Acquisition, Organizational Policy
Holistic "End-to-End" IT Systems	Limited and Focused IT Services	Security, IT Infrastructure Design, Resource Management, IT Procurement & Acquisition, IT Operations, Organizational Policy

The impact on the IT workforce is also significant and will require the IT professional to change, notes Jay Kerley, Vice President and Deputy CIO at Applied Materials. They need to go from "doing" to "managing" or face obsolescence. Dr. Richardson noted that the "most critical limitation is finding appropriately trained people. Cloud computing requires a very different type of IT person—more flexible and innovative—but they are hard to find, especially with TS/SCI." As the use of cloud computing expands, the human resources necessary for managing security settings, role-based access, network changes, and technology changes will also increase. There is also a need for non-technical employees to be familiar with this technology because although it is perceived that the benefits of this process largely revolve around "tech issues" such as data analytics and server efficiency, the perceived risks are to the mission. The Lockheed Martin report, *Awareness, Trust and Security to Shape Government Cloud Adoption* states, "There are many awareness gaps among professionals who will be investigating, implementing, using, securing and managing cloud computing. Conversely, this data may also suggest that implementing and managing cloud computing platforms within federal agencies will require cross-functional discussion among both IT policy and IT implementation professionals."[11]

CLOUD COMPUTING WILL NECESSITATE, AND FORCE, ACQUISITION REFORM

An observation made in study after study is that acquisition cycles for most IT in the national security space are much too long. The serious problem posed by acquisition length was noted in the DoD's recent *Strategy for Operating in Cyberspace*. Traditionally, the adoption pace for IT is seven to ten years, and the need to shorten the cycle is explained in the report: "To replicate the dynamism of the private sector and harness the power of emerging computing concepts, DoD's acquisition processes for information technology will need to address speed as a critical priority. DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years."[12] It is widely believed that cloud enables agility and accelerates time to market. A senior government official involved in enterprise system development voiced concern that Federal Acquisition Regulation must change to deliver consumer services, as it is not currently structured to support a business model shift to cloud computing.

Federal Acquisition Regulation must change to deliver consumer services, as it is not currently structured to support a business model shift to cloud computing.

One view was that "government agencies can go at it alone." Purpose-built computing may be ideal to support the highest levels of security standards for government cloud computing environments. There is a need for a model that balances acquisitions for internal purposes and outsoures services to a cloud provider. Cloud solutions already developed for private consumers may be realigned to fit government-specific models. Following the industry trend to move from performing IT services to managing SLAs allows for specialization in areas that relate business advantages to economies of scale by capitalizing on proficiency and subject matter expertise. Our perception, based on these interviews, is that improvements in how agencies acquire services, software, and hardware are strongly desired by most involved in the implementation of cloud computing, and many believe that the adoption of cloud solutions may actually catalyze and accelerate those needed improvements.

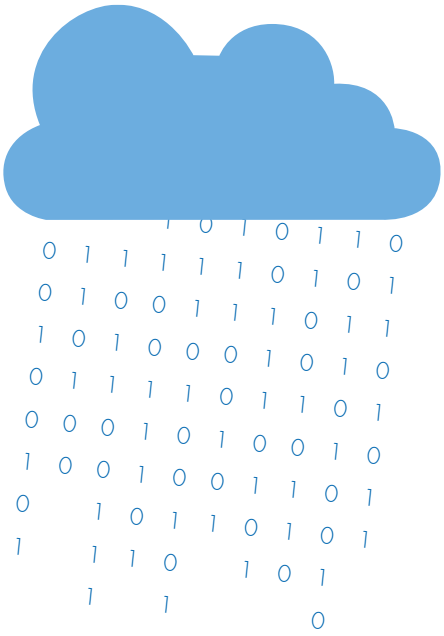
CLOUD COMPUTING WILL REQUIRE THE FORMULATION OF NEW STANDARDS

In the corporate world, many companies realize too late that moving to a cloud architecture does not remove all integration issues. One must never assume that cloud models are easier to integrate. In fact, there are times when integration issues between various systems may become more complex. Today's resource management culture does not yet take into account how cloud computing really works; for example, most people forget that terminating an old process is required to manage the cloud life cycle more effectively. Budgeting and accounting will be difficult unless this aspect of cloud resource management is changed. This is seen as one of the biggest hurdles for organizations looking to adopt cloud computing.

The government needs to look for standards that have traction and are being implemented. Some standards are being rushed out ahead of time, and some standards bodies are holding back. Some standards take too long to develop, perhaps decades or even longer. However, there was a consensus in the private sector that the government must eventually adopt open standards, at the peril of vendor lock-in. As in the past, the NSA, NIST, NASA, and other agencies have participated in software standards committees, and the government should continue to be involved in the formulation of cloud computing standards. The risk here is that by adhering to a standard now, the organization may miss out on innovation. One CTO explained that the danger with any new technology is that if you standardize too early you face the reality that standards are determined by vendors or providers, not by users. It is possible that certain standards may limit the scale or security of the underlying cloud technology.

Many surveyed agreed that there are not any de facto standards that cloud computing providers have settled upon. Without standards, you cannot scale. Standards bring consistency, critical mass and, eventually, specialization in terms of service delivery. Until clarity on general standards emerges, the government is playing roulette and needs to hedge its bets. It could decide on initial standards, but include the ability to support multiple standard contenders as necessary. Within this virtual "survival of the fittest" environment, it is difficult to pick the winners up front. It is an organic process. If you need to pick a "winner," then have a contingency plan to move to a new standard. It does appear that viable standards for federal cloud computing are emerging, but effective organizational leadership will be required to ensure that enhanced security and cost efficiencies will be realized.

Clouds do not automatically solve any information sharing policy or cultural challenges. Implementation will require the government to evolve certification and accreditation processes and revamp outdated systems. According to a senior technology professional at NSA, there are no technical barriers to the IC arriving at a community-wide approach to cloud computing, but this adoption may require agencies to overcome substantial integration issues. Diligence must be exercised when moving forward with a cloud implementation, but there will always be a certain measure of risk and uncertainty involved.



III. CONCLUDING THOUGHTS

The advent of cloud computing represents a powerful trend that promises to change the landscape of the IC. Beyond its technological functions, the cloud computing model expands access to the power of information technology while potentially reducing operations and sustainment costs. The IC will benefit from an informed approach to cloud computing adoption, but should be aware that these deployments are not a panacea. They do not inherently solve the significant information sharing and cultural challenges noted by senior executives in the IC. They may, however, catalyze discussion on shifting business processes to enable smart change.

If successfully implemented and managed, cloud computing approaches and technologies can revolutionize the IC's computing capabilities by more efficiently and effectively enabling the majority of IC functions.

Our key conclusions bear repeating here:

- **Cloud computing is not simply the consolidation and virtualization of software and systems, but a change in an organization's business model.**
- **Migration to a cloud model should be primarily focused on improving mission accomplishment.**
- **The type of cloud deployment depends on the security protection needed for the data involved.**
- **Cloud computing is more about long term cost avoidance and support to the mission than immediate cost reduction.**

Cloud computing should be seen as a new way of doing business that will transform an organization's policies and processes. While studies indicate cost savings are not likely to come from cloud adoption alone, cost avoidance is likely, and implementing cloud architectures may facilitate consolidation that can generate savings. However, this will only occur with careful planning and design. If successfully implemented and managed, cloud computing approaches and technologies can revolutionize the IC's computing capabilities by more efficiently and effectively enabling the majority of IC functions. This wave of innovation will change the way IT resources are consumed and how missions are accomplished. Cloud computing even has the potential to generate revenue for the government in the long run as the largest content provider on the planet. As cloud computing innovations are adopted we expect to see improvements in security and IT efficiency, but only if end-to-end requirements, designs, and architectures are carefully considered. Guidance from the IT industry, the private sector, and academia must inform and drive decision-making in this sphere. Many public and private organizations are learning valuable lessons independently, but new ways of partnering across government, academia, and industry must be piloted to ensure continuous, productive cooperation and reduce risk. Interaction and execution amongst these sectors and in support of government will ensure the successful transition of the Intelligence Community to the cloud.

INTERVIEW PARTICIPANTS

INDUSTRY

Kerry Bailey, *Group President of Cloud Strategy and Services, Verizon Business* (currently Chief Marketing Officer at Verizon Enterprise Solutions)*

Simon Crosby, *Chief Technology Officer and Co-founder, Bromium*

Bill Cullen, *Chief Technology Officer, AppZero* (currently Principal at Whitecap Development)*

Dave Cullinane, *Chief Information Security Office, eBay, Inc.*

Christopher Ferris, *Distinguished Engineer and Chief Technology Officer of Industry Standards in the Software Group Standards Strategy Organization, IBM Corporation*

Jay Fry, *Vice President of Marketing for Cloud Computing, CA Technologies*

Brian Goodman, *Manager of Advanced Cloud Technology, Master Inventor, and Senior Technical Staff Member, IBM Corporation*

Rod Johnson, *Senior Vice President of Application Platform Strategy, VMware; Chief Executive Officer, SpringSource*

EJ Jones, *Technical Fellow in Information Security, Boeing*

Jay Kerley, *Corporate Vice President and Deputy Chief Information Officer, Applied Materials*

Dustin Kirkland, *Engineering Manager, Canonical* (currently Chief Architect at Gazzang, Inc.)*

Victoria Kouyoumjian, *IT Strategies Architect, ESRI*

Haden Land, *Vice President and Engineering & Chief Technology Officer, Lockheed Martin IS&GS Civil*

Marwa Mabrouk, *Managed Services Technical Lead, ESRI*

Donald Norbeck, *Acting Chief Technology Officer, VCE* (currently Technology Officer for Virtualization, Cloud Computing, and Product Strategy at SunGard Availability Services)*

Eric Olden, *Chairman and Chief Executive Officer, Symplified, Inc.*

Ken Owens, *Vice President of Security Technology, Savvis Communications* (currently Technical Vice President at Savvis)*

Gregor Petri, *Senior Director EMEA Marketing, CA Technologies* (currently Research Director at Gartner)*

Jon Ramsey, *Executive Director of Development Engineering at SecureWorks, Dell*

Edward Screven, *Chief Corporate Architect, Oracle*

Fran Trentley, *Senior Director, Akamai Technologies*

Bill Vass, *President and Chief Executive Officer, Liquid Robotics*

Rick Wolski, *Chief Technology Officer, Eucalyptus Systems, Inc.*

GOVERNMENT

Keith Barber, *Implementation Lead for Online On-Demand Services, NGA*

Major Kris Barcomb, *United States Air Force*

Rob Brunngraber, *IT Acquisitions, NGA*

Gus Hunt, *Chief Technology Officer, CIA*

Jan Janssen, *Director of the Ground Enterprise Directorate, NRO*

Mark Kuzma, *Chief Architect, Maritime ISR Enterprise, Hopper Information Services Center – (ISC-T), ONI*

Rick Ledgett, *National Intelligence Manager for Cyber, ODNI*

Jim Richberg, *Deputy National Issue Manager for Cyber, ODNI*

Dr. Russell Richardson, *Chief Architect, INSCOM; Senior Vice President, Sotera Defense Solutions*

Dr. Pete Rustan, *Director Of Mission Support Directorate, NRO*

Jill Singer, *Chief Information Officer, NRO*

Joe Smith, *Technical Executive, NGA Acquisition Directorate, Sensor Assimilation Division (ASX), NGA*

Al Tarasiuk, *Associate Director of National Intelligence and Chief Information Officer, ODNI*

Neill Tipton, *Director of Information Sharing and Partner Engagement, DoD*

Keith Trippie, *Executive Director of Enterprise System Development, DHS*

Lieutenant General Richard Zahner, *Deputy Chief of Staff, G-2, United States Army*

Participation in the interviews does not imply personal or official endorsement of the views in this paper by either the interviewee or his/her office.

**Position during the interview process.*

ENDNOTES

[1]"Jeff Bezos' Risky Bet." Bloomberg Businessweek. November 13, 2006.

[2]Cloud bursting: an organization's ability to shift additional workloads to an external (public) cloud on an on-demand basis.

[3]GAO, Testimony Before the Committee on Oversight and Government Reform and Its Subcommittee on Government Management, Organization, and Procurement, House of Representatives, "Information Security: Government-wide Guidance Needed to Assist Agencies in Implementing Cloud Computing." July 1, 2010.

[4]Cooke, Jim. "The Shift to Cloud Computing: Forget the Technology, it's about Economics." Cisco Internet Business Solutions Group. December 2010.

[5]"Technology Avalanche," David Evans, Cisco Internet Business Solutions Group, 2010.

[6]Clark, Jeffrey. "Federal IT Consolidation: The Show Goes On." The Data Center Journal.

[7]Marks, Joseph. "If You Think You'll Save Money with Cloud Computing, Think Again." Nextgov. Dec 6, 2011.

[8]Jackson, Kevin. "Implementation of Cloud Computing Solutions in Federal Agencies: Part 4 - Cloud Computing for Defense and Intelligence." Forbes, August 31, 2011.

[9]Awareness, Trust and Security to Shape Government Cloud Adoption." Lockheed Martin, 2010. P 1.

[10]Babcock, Charles. "Virtualization Pioneers Crosby, Pratt Tackle Cloud Security." InformationWeek. 22 June 2011.

[11]Awareness, Trust and Security to Shape Government Cloud Adoption." P 1.

[12]Department of Defense Strategy for Operating in Cyberspace, July 2011.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 160 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
SUPPORTING ADVANCES IN THE NATIONAL SECURITY AGENDA

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org