

WHITE PAPER

# Getting Secure in the Cloud

*How to Meet IT Mandates,  
Ensure Security and  
Achieve Cost Savings for  
Your Government Agency*

JULY 2011



LM CYBER SECURITY™  
**ALLIANCE**

**LOCKHEED MARTIN**   
*We never forget who we're working for®*

**MARKET CONNECTIONS, INC.™**  
Research You Can Act On

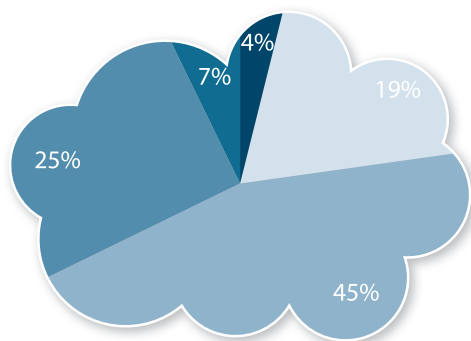


## Summary

The landscape is improving for cloud computing initiatives and adoption by federal agencies, though security issues and concerns continue to cause hesitation for decision-makers, according to the Lockheed Martin Cyber Security Alliance survey on cloud computing and cyber security conducted by Market Connections, Inc. A similar survey conducted last year

indicated that the more aware and involved government IT decision makers were with cloud computing and cyber security in general, the more they trusted the cloud model.<sup>1</sup> That pattern continues this year: three out of five study participants trust cloud computing and believe it is appropriate for at least some applications.

Three out of five study participants trust cloud and believe it is appropriate for at least some applications.



Trust ■■■■ No Trust

It is at the intersection of applications and security that concerns arise. Just over three-quarters of respondents believe some data are simply too sensitive to place in the cloud, which in turn leads to limits on which applications are appropriate for a cloud environment. Half of the respondents said that demonstrating cloud security is the number one thing service providers can do to increase federal agencies' confidence in their solutions.

The creation of a 25-point plan for moving to the cloud by the Office of Management and Budget (OMB) is credited with shifting agencies toward "cloud-first" IT solutions. Still, half of the respondents either have no idea or expressed no opinion whether the timeline for cloud implementation in the OMB plan is a guideline or a requirement.

This white paper:

- ▶ Provides a snapshot view of the degree and type of cloud computing adoption in federal government agencies;
- ▶ Reports trust levels related to cloud computing and different delivery models;
- ▶ Identifies specific cloud computing and cyber security concerns and policy measures being taken to address those concerns;
- ▶ Presents conclusions that can be drawn from the study data and recommendations to help government agencies prepare to adopt, secure and manage cloud computing.

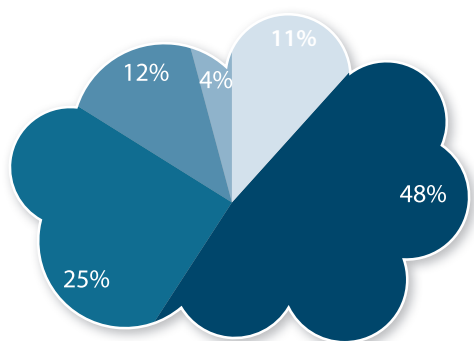
<sup>1</sup> "Awareness, Trust and Security to Shape Government Cloud Adoption," Lockheed Martin Cyber Security Alliance and Market Connections Inc., April 2010.



## Security Awareness in the Cloud

As cloud computing moves toward broad-based acceptance with federal contractors, federal agencies also are moving to embrace it, though individual professionals may not be aware of the change. While 41 percent of contractors say that the agencies they work for have adopted cloud-based solutions to date, only 34 percent of federal employee respondents said they have moved applications to the cloud.

Only 34% of federal government respondents said they have moved applications to the cloud.



- All for cloud for everything
- Cloud OK for some things
- Not yet sold on cloud
- Cloud idea is disconcerting
- Not in favor of cloud

A major reason for the gradual pace of adoption is that nearly all participants in the study said security is an essential element they look for in a cloud solution. In fact, two-thirds indicated this is the most important element in their evaluations.

Concerns about security in the cloud are reflected in several ways. Nearly half of the participants gave a neutral rating when asked how much they trust cloud computing, four out of 10 participants said their agency is likely to use a private cloud, while half said they would be likely to use a federal community cloud.

At the same time, those familiar with cloud are more than twice as likely to trust cloud-based solutions, with 57 percent versus 24 percent.

Also, nearly half of participants indicated they are willing to use cloud computing for some applications, but not others. Sensitivity to which applications are cloud-suitable is based on security concerns — three-quarters of participants agreed that some data is too sensitive to have in the cloud.

At the same time, 11 percent agreed that cloud-based computing is a good solution for all data and applications and another one-quarter could be sold on the idea with a bit more information. This indicates that if security concerns can be addressed successfully, the cloud would be embraced unreservedly by a number of agencies.

**“Security is the most important feature and the reliability of the cloud depends on it.”**

DIVISION CHIEF



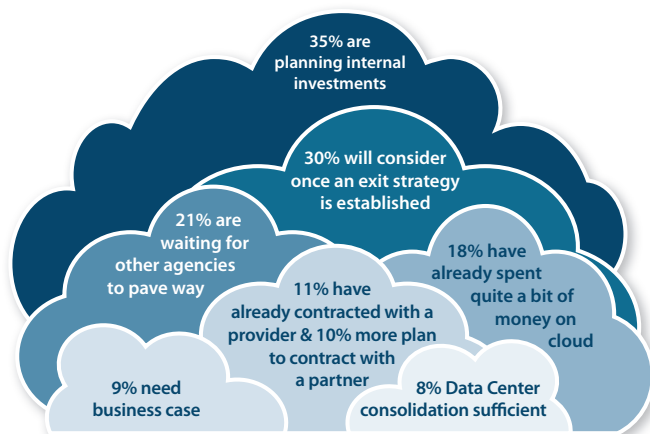
## Other Prerequisites for Cloud Computing

The concerns about security identified by study participants are not the only obstacles holding back federal agencies moving to the cloud. At least three-quarters of respondents identified dependability, availability, and the ability to continue using existing applications as elements that cloud-based solutions must address.

The concerns about security identified by study participants are not the only obstacles holding back federal agencies moving to the cloud. At least three-quarters of respondents identified dependability, availability, and the ability to continue using existing applications as elements that cloud-based solutions must address.

As federal agencies deal with the reality of tight budgets, the prospect of saving money by moving to cloud computing is appealing. More than one-third of respondents say they are well into planning internally to make the move, including budgeting the necessary investment dollars. Despite the cost saving incentives, half the participants indicated that although their agency is talking about moving applications to the cloud, they have not taken any steps to make the transition. Nearly one in ten say they need the business case to be made to justify moving forward with cloud, while eight percent stated they do not believe there is a reason to go further than data center consolidation. A small number of respondents, approximately two percent, agreed with both statements.

Planning for eventualities is important, too. One-third say they will consider more seriously the prospect of cloud computing once they have an exit strategy, in case it does not work the way they envision, and one-quarter say they are waiting for other agencies to take the lead in making the transition.



**“Before you can invest, you’ve got to have a plan. The number of cloud solutions that meet federal standards is quite limited.”**

ASSOCIATE DIRECTOR

**“We are unsure how communication is routed within the cloud and the lack of information is what creates discomfort.”**

CHIEF OF IT



## Deployments and Applications

---

Compared with Software as a Service (SaaS), fewer agencies have deployed Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or IT as a Service (ITaaS), but at least one-third of agencies are discussing deployment of these in a cloud environment.

There are many ways for agencies to approach implementing cloud computing solutions. For instance, approximately one-third of respondents said their agencies have fully or partially deployed Software as a Service (SaaS) in the cloud, and an additional 54 percent are either discussing deployment or already have a plan in place for deployment. By comparison, fewer agencies have deployed Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or IT as a Service (ITaaS), but at least one-third of agencies are discussing deployment of these in a cloud environment.

The applications identified by more than 60 percent of the participants as either already moved or most likely to be moved to a cloud environment include enterprise resource planning (ERP), document creation, document management, virtualized server environments, customer resource management (CRM) and Web applications. Other applications that were mentioned for possible movement to a cloud environment include Voice over IP (VoIP) and e-mail.

More than one-quarter of participants identified mission-critical data management, procurement, human resource management and financial management systems as applications they would never consider moving to the cloud, reflecting concerns about cloud security.

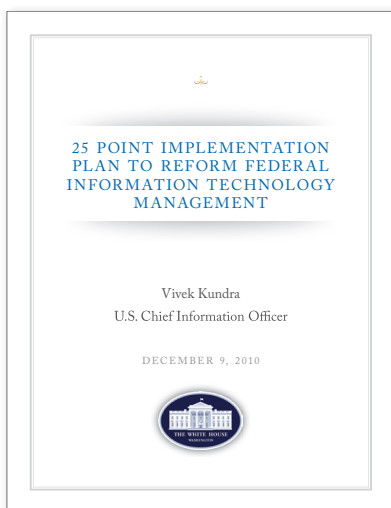
**“Currently our exchange server, travel and payroll software and staff data storage is in the cloud. Our intranet is also cloud-based. We are in the process of moving all of our internal apps into the cloud.”**

CHIEF OF INFORMATION TECHNOLOGY



## Impact of the “25-Point Plan”

In December 2010, the Office of Management and Budget’s CIO, Vivek Kundra, released his “25-Point Plan” for information technology, telling agencies they must first consider cloud-based services for their IT needs (or risk losing funding for new IT investments). By June 2011, agencies across the government had identified 78 IT services to be moved to the cloud by the end of the year. OMB expects agencies to relocate two additional services each to the cloud by June 2012.<sup>2</sup>



Despite that plan, one-half of respondents either admitted they have no idea, or gave a neutral response when asked if they agree that the timeline for cloud implementation in the plan is a guideline, not a mandate.

The Federal CIO Council has been tasked with creating a government-wide Risk and Authorization Management Program (FedRAMP), to provide joint security assessment, authorizations and continuous monitoring of cloud computing services for all federal agencies. From the Draft Executive Summary:

“The decision to embrace cloud computing is a risk-based decision, not a technology-based decision. ... Once the business decision has been made to move towards a cloud computing environment, agencies must then determine the appropriate manner for their security assessments and authorizations.”

*Proposed Security Assessment and Authorization for U.S. Government Cloud Computing, CIO Council, Draft Version 0.96, Nov. 2, 2010.*

Agencies are seeking tangible proof of secure cloud applications. Half of the respondents said that demonstrating cloud security is the number one thing service providers can do to increase federal agencies’ confidence in their solutions. Every other measure to increase federal comfort levels was in the single digits; adhering to standards and certifications, ensuring reliability and stability of cloud applications, and education each were mentioned by six percent of respondents.

**“...It is cost savings that are a main reason for going to the cloud. But realistically, failure to meet the other qualities mentioned (reliability, scalability) would be highly detrimental as well.”**

ASSOCIATE DIRECTOR

<sup>2</sup> “OMB twists arms to push cloud projects,” Federal Times, June 12, 2011.



## Changes Over 12 Months

Last year, 14 percent of respondents reported their agencies had moved one or more applications to the cloud. This year that has increased to 34 percent.

The 2011 study showed a 20 percentage-point increase in migration of applications to the cloud.

At the time of last year's study, 12 percent were discussing moving one or more applications to the cloud but had not yet done so. This year, 50 percent are having those discussions.

Headway continues, with study results revealing increased knowledge and familiarity with agencies' plans for moving to cloud computing. Last year, 57 percent of respondents were not familiar with the concept (now 34 percent) or unsure if their agency used the cloud (23 percent). In this year's study, only five percent are unsure of the status of their agency moving applications to the cloud.

Perhaps most striking in this year's study is the degree to which agencies are considering moving specific applications to the cloud. For many applications, such as ERP, CRM, and virtualized server environments, evaluation of suitability for cloud is underway by 70 percent or more of the respondents.

While still under consideration by more than half the respondents, other applications, most notably procurement and human resources management, are not seeing such sharp increases, perhaps because they are seen as more vulnerable to potential security breaches.

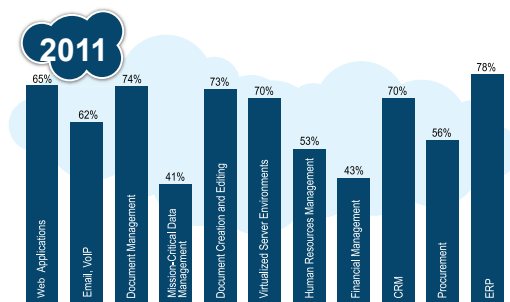
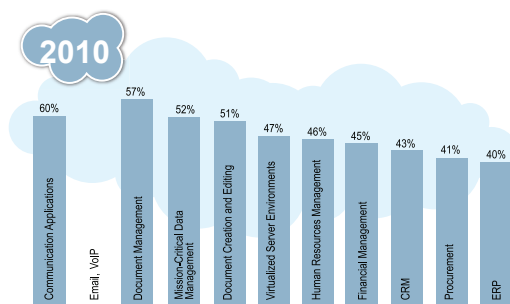
While there appears to be lower resistance to moving some applications to the cloud, last year, 52 percent of respondents said they were considering moving "mission critical data" to the cloud. This year, only 41 percent expressed that view. Moving financial management applications and data to the cloud also continues to meet with resistance — 43 percent of respondents this year said they would be less likely to consider it compared to 45 percent last year.

Growing familiarity with the concept of cloud computing and understanding of its advantages also is reflected in lessening concerns about security. Those who are more familiar or involved with cloud computing are less concerned about security (57 percent this year, versus 67 percent in 2010).

Despite the expanding familiarity with cloud, federal community (49 percent) and private (41 percent) clouds continue to be the most desired deployment modes for agencies.

**"We are consolidating our systems and creating a private cloud."**

ASSISTANT DIVISION CHIEF





## Conclusions and Recommendations

Cloud computing is making rapid gains in acceptance by federal agencies, driven in large part by growing familiarity with the concept and increased involvement with implementation. The more agencies work in the cloud, the greater their level of acceptance becomes for expanding the applications.

Agencies are motivated to make the transition to the cloud by OMB policy requirements and pursuit of cost savings. Security concerns continue to challenge cloud adoption, particularly with regard to applications that rely upon mission-critical data.

Government agencies are eager for demonstrations of secure cloud applications, though they continue to express a preference for private clouds. Many federal agency IT professionals are looking for others to make the change first and share their cloud implementation experiences and lessons learned. Additional education about what goes on in the context of clouds, providing greater transparency about their operations and information about standards, will go a long way to break down barriers and accelerate adoption.

With the cloud landscape changing so rapidly, it is recommended that organizations take the following actions when developing plans for implementation of cloud solutions:

- ▶ **First, clearly define what cloud means to your organization.** Having a common definition of what a cloud is and what cloud computing means for your agency specifically will make it much easier to manage cloud initiatives, including planning, implementation and security.
- ▶ **Reach out to IT professionals in other agencies to ask about their experiences with cloud.** There are numerous cloud initiatives under way in both civilian and defense agencies, and many individuals are willing to share their lessons learned and best practices.
- ▶ **Engage professionals from organizations with specific cloud security expertise.** Every agency has mission-critical data to protect and it rarely requires a custom security solution. As with all IT projects, it is much easier (and more secure) to “bake in” security protections at the start of a project than to add them as an overlay at the end.
- ▶ **Take a broad view when considering cloud security.** Cloud computing can have implications that security professionals may not have considered. Also, overall security policies need to extend to users accessing applications in the cloud and via traditional methods. Systems, staff, training, and policies should be assessed and adjusted as needed to support cloud computing effectively.
- ▶ **Move beyond the mandate to adopt cloud computing.** Develop an internal vision of the role that cloud computing will play in meeting the agency’s mission, including (but not limited to) cost savings that will enable other IT projects, and share it throughout the organization.



## About the Study

Market Connections, Inc. conducted a study in two phases for Lockheed Martin's Cyber Security Alliance to measure attitudes, awareness, level of comfort and trust with security and cloud computing.

The first phase of the study comprised in-depth interviews, which helped to shape the online survey questions during phase two. The 196 study participants are all involved with IT security solutions and have some level of familiarity with their agency's cloud computing initiatives.

Study participants represent all branches of the federal government and military services, and several intelligence agencies. Federal government contractors were invited to participate as over the past year more and more IT services are being outsourced.

## About the Lockheed Martin Cyber Security Alliance

The Lockheed Martin Cyber Security Alliance combines the strengths of market leading companies' solutions and integrates their best practices, hardware, software, and tools within a unique new research, development and collaboration center called the NexGen Cyber Innovation and Technology Center. The alliance companies include: APC by Schneider Electric, ArcSight, CA, Cisco, Dell, EMC Corporation and its RSA security division, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, Symantec, Trustwave and VMware.

## About Lockheed Martin Corporation

Headquartered in Bethesda, Md., Lockheed Martin is a global security company that employs about 126,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services. The Corporation's 2010 sales from continuing operations were \$45.8 billion. *For more information visit: [www.lockheedmartin.com](http://www.lockheedmartin.com).*

## About Market Connections, Inc.

Celebrating its 15th anniversary this year, Market Connections provides comprehensive B2B and B2G market research services, enabling organizations to make informed, intelligent decisions that drive significant and measurable business and process improvements. The firm offers deep domain expertise in numerous markets, including federal, state and local governments; information technology and telecommunications; education; healthcare; and associations and non-profits. *For more information visit: [www.marketconnectionsinc.com](http://www.marketconnectionsinc.com).*

LM CYBER SECURITY™  
**ALLIANCE**

**LOCKHEED MARTIN**  
*never forget who we're working for®*

**MARKET CONNECTIONS, INC.™**  
Research You Can Act On