THE WRIGHT FLYER PAPERS

# The Department of Defense and the Power of Cloud Computing

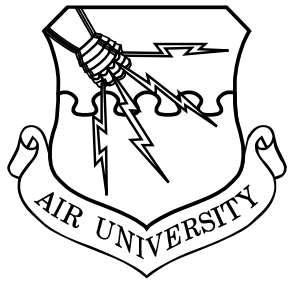
## Weighing Acceptable Cost versus Acceptable Risk

Steven C. Dudash
Major, Ohio Air National Guard

Air Command and Staff College
Wright Flyer Paper No. 52

Please send inquiries or comments to
Editor
*The Wright Flyer Papers*
Department of Research and Publications (ACSC/DER)
Air Command and Staff College
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426
Tel: (334) 953-3558
Fax: (334) 953-2269
E-mail: acsc.der.researchorgmailbox@us.af.mil

AIR UNIVERSITY
AIR COMMAND AND STAFF COLLEGE




# The Department of Defense and the Power of Cloud Computing

## Weighing Acceptable Cost versus Acceptable Risk

Steven C. Dudash
Major, Ohio Air National Guard

Wright Flyer Paper No. 52

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

*Project Editor*
James S. Howard

*Copy Editor*
Carolyn Burns

*Cover Art, Book Design, and Illustrations*
Daniel Armstrong
L. Susan Fair

*Composition and Prepress Production*
Nedra O. Looney

*Print Preparation and Distribution*
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

*Director and Publisher*
Allen G. Peck

*Editor in Chief*
Oreste M. Johnson

*Managing Editor*
Demorah Hayes

*Design and Production Manager*
Cheryl King

Air University Press
155 N. Twining St., Bldg. 693
Maxwell AFB, AL 36112-6026
afri.aupress@us.af.mil/

http://aupress.au.af.mil
http://afri.au.af.mil/

Published by Air University Press in April 2016




This Wright Flyer Paper and others in the series are available electronically at the AU Press website: http://aupress.au.af.mil/

## Contents

# Illustrations

*Table*



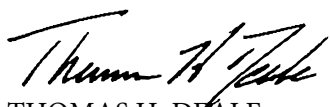
*Figure*

# Foreword

It is my great pleasure to present another issue of *The Wright Flyer Papers*. Through this series, Air Command and Staff College presents a sampling of exemplary research produced by our residence and distance-learning students. This series has long showcased the kind of visionary thinking that drove the aspirations and activities of the earliest aviation pioneers. This year's selection of essays admirably extends that tradition. As the series title indicates, these papers aim to present cutting-edge, actionable knowledge—research that addresses some of the most complex security and defense challenges facing us today.

Recently, *The Wright Flyer Papers* transitioned to an exclusively electronic publication format. It is our hope that our migration from print editions to an electronic-only format will fire even greater intellectual debate among Airmen and fellow members of the profession of arms as the series reaches a growing global audience. By publishing these papers via the Air University Press website, ACSC hopes not only to reach more readers, but also to support Air Force–wide efforts to conserve resources. In this spirit, we invite you to peruse past and current issues of *The Wright Flyer Papers* at http://aupress.maxwell.af.mil/papers_all.asp?cat=wright.

Thank you for supporting *The Wright Flyer Papers* and our efforts to disseminate outstanding ACSC student research for the benefit of our Air Force and war fighters everywhere. We trust that what follows will stimulate thinking, invite debate, and further encourage today's air, space, and cyber war fighters in their continuing search for innovative and improved ways to defend our nation and way of life.



THOMAS H. DEALE
Brigadier General, USAF
Commandant

## About the Author

Maj Steven C. Dudash is the director of logistics for the 251st Cyberspace Engineering Installation Group. He began his military career as an enlisted wideband communications equipment specialist in March 1987, and earned his commission through the Academy of Military Science, the Air National Guard commissioning program, in 2001. He holds a bachelor of science degree from Franklin University and a master of military operational art and science degree from Air University.

## Abstract

Cloud computing, a shared pool of computing resources that are readily available to meet the user's rapidly changing demands, has opened up many new opportunities and risks for society that in many ways are revolutionary. The Department of Defense (DOD), because of its size and mission, faces significant opportunities and security challenges when implementing a cloud computing environment. The transformation of DOD information technology (IT) has been uneven as the technology has matured. A cloud-based infrastructure can provide extensive savings for the DOD. Currently, there is an estimated 75 percent underutilization rate in current configurations. However, a cloud configuration introduces new potential security risks that DOD IT professionals must weigh when evaluating the potential cost savings associated with cloud computing.

The implementation of a private DOD cloud—an infrastructure solely owned and operated by the DOD supporting all DOD components—could realize savings while reducing or eliminating the risks associated with cloud computing. This paper evaluates existing policy, guidance, law and regulation, and recent efforts within the DOD to implement a cloud-computing infrastructure. There are three key recommendations for the DOD's transformation to make the most of cloud computing: standardize security categorization, implement a DOD private cloud, and evaluate the most cost-effective commercial cloud solutions with the least security risk.

# The Problem

> *Complete confidence in the trustworthiness of information technology, users, and interconnections cannot be achieved; therefore the Department of Defense must embrace a risk management approach that balances the importance of the information and supporting technology to DOD missions against documented threats and vulnerabilities, the trustworthiness of users and interconnecting systems, and the effectiveness of IA solutions.*
>
> Department of Defense Instruction 8500.2

The Department of Defense (DOD) spends over 38 billion dollars per year on information technology (IT) supporting over two million users and 10,000 operational systems.[1] As the US Congress looks to decrease the DOD budget in order to achieve a balanced budget, the DOD must look at methods to live within its budget and still meet mission requirements. At 38 billion dollars per year, IT becomes an obvious target for savings.

The US chief information officer (CIO) published the December 2010 *25 Point Implementation Plan to Reform Federal Information Technology Management*, which called for a "cloud first" approach in implementing IT infrastructure.[2] The 2012 *National Defense Authorization Act* (*NDAA*) calls for DOD data and services to be migrated to the commercial cloud infrastructure. It fails to provide clear guidance on the approach federal agencies should take in supporting this "cloud first" directive, however.[3] The *NDAA* does not provide guidance on how to identify the proper mix of commercial and private cloud infrastructure while maintaining the proper level of security for the infrastructure, services, and data. While clouds are an industry-proven way to reduce IT infrastructure and therefore cost, this migration must not be done in a manner that places the DOD data at risk.

According to the National Institute of Standards and Technology, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[4] This complex definition of cloud computing does little to highlight the key benefits as well as the key security risk of cloud computing: "shared pool." From a user's perspective, this shared pool of resources is a "cloud" of unknowns. The user does not know

where the supporting IT resources supporting reside and what the laws and regulations concerning data availability and privacy are at that location. The user may have no knowledge with whom the resources are shared and, therefore, has no knowledge of the security process utilized by these neighbors in the cloud. A neighbor practicing security standards lower than that of the DOD will put DOD systems and data at a risk level comparable to that of their neighbors in the cloud. Just as a user browses a Web page on the public Internet and may not know the identity and location of the host, so too a user may face similar unknowns about the cloud. However, it is this shared pooling of resources that provides one of the greatest benefits of cloud computing—economies of scale. According to John K. Waters, writing for the award-winning *CIO.com*, "the average enterprise utilizes somewhere between 5 percent and 25 percent of its server capacity."[5] Unfortunately, it is this shared pool of resources, especially shared resources in a commercial environment, that also creates numerous risks not usually seen in the traditional client / server IT models.

Without overall federal guidance, the DOD and its three military components have been left to their own devices to develop their cloud strategy within their assigned budgets. The DOD waited over 18 months after the US CIO published the "cloud first" policy to establish its first strategic guidance. That guidance came after the initial deadline for the components had passed.

As a result, the three military components have established three different paths to achieve a cloud presence. While the benefits of cloud computing are increasingly understood, by failing to work as a single organization, the DOD does not take advantage of economies of scale. It seems to be unable to adequately address elevated security risks posed by commercial cloud infrastructure. Consequently, individual DOD components and agencies are developing different cloud strategies independently. Then the question becomes, How should the DOD implement a shared pool of configurable computing resources (a cloud computing environment), ensuring savings through economies of scale while adequately protecting the DOD's data and services?

The DOD should build and mandate the use of a DOD private cloud computing environment able to provide core IT services and data storage for all DOD components in order to accomplish its strategic objectives on cloud computing. This type of infrastructure can achieve significant economies of scale across the entire DOD while minimizing the risks associated with cloud computing.

Both the problem / solution and the evaluation methodologies will be utilized to find an acceptable combination of commercial public cloud service with DOD private cloud service that provides cost savings and

required levels of system and data security. By analyzing the cloud infrastructure, legal requirements in cloud computing, data security requirements of the Federal Information Processing Standards (FIPS), and operational considerations, several potential cloud model alternatives will be presented. Looking at "commercial only," "private only," and "hybrid" models, the strengths and weakness of each will be shown. Finally, a series of recommendations will be presented that should allow the DOD to achieve economies of scale through the power of cloud computing while still ensuring adequate protection to the systems and data.

## Understanding Cloud Computing

As stated earlier, the goal of cloud computing is to create a rapidly configured, on-demand, shared pool of resources. It is through these goals that cloud computing has the potential to provide a cheaper, hands off, more secure IT infrastructure. The first of these benefits, cheaper infrastructure, is provided by economies of scale. Tim Hindle in the *Economist* defines "economies of scale" as "factors that cause the average cost of producing something to fall as the volume of its output increases."[6] If the DOD applies the proposed cloud computing concepts, DOD IT infrastructure could be consolidated from numerous inefficient data centers to fewer, more efficient, large-scale data centers, which would increase output—economies of scale.

The "hands off" benefit of cloud computing depends on perspective, whether that of the user, the business, or the cloud provider. This paper will focus on the business perspective—that is, the point of view of the organization providing goods or services and requiring IT services to meet those needs. The businesses would include the military components and agencies of the DOD. Ignoring the newer realm of cyber operations and focusing on the IT services required by the DOD—what does cloud computing bring to businesses? According to Salesforce.com, a commercial cloud provider, "With cloud computing . . . you're not managing hardware and software—that's the responsibility of an experienced vendor like Salesforce.com. The shared infrastructure means it works like a utility: You only pay for what you need, upgrades are automatic, and scaling up or down is easy."[7] From a component or agency perspective, a DOD private cloud will allow a hands-off approach to the cloud with a core business focus.

The third benefit of cloud computing, more secure IT infrastructure, occurs through the consolidation of similar services. Recently, the Defense Information Systems Agency (DISA) was able to halt the spread of a malware attack on the DOD private cloud e-mail services because it was possible to view the entire process, not just its pieces. Mark Orndorff,

DISA's director of mission assurance and network operations, stated that "those attacks would have been essentially undetected if you just had little pieces of that picture scattered around the DOD cyber workforce."[8] This paper will also show the new security issues lurking in the shadows of cloud computing.

Just as clouds in the sky take on many different shapes and sizes, the benefits of cloud computing described above can be delivered through clouds of many different shapes and sizes. A cloud environment is known by its implementation model and by the services that it provides—information as a service (IAAS), platform as a service (PAAS), or software as a service (SAAS). Regardless of the model or service selected, the process of implementing a cloud-computing environment starts with server virtualization.

## Virtualization

To use a very generic definition of server virtualization, "a virtual server mimics, using software alone, the behavior and capabilities of a stand-alone computer."[9] One of the first physical steps taken in the migration from a traditional IT infrastructure to a cloud computing environment, virtualization also provides many of the benefits called for in the 2012 *NDAA*. David Marshall, an architect of numerous virtual solutions and writer for *Infoworld*, has identified the top 10 benefits of server virtualization:

- energy savings,
- data center footprint reduction,
- quality assurance / lab environments,
- faster service,
- hardware vendor lock-in reduction,
- uptime increase,
- improved disaster recovery,
- application isolation,
- life extension of older applications, and
- help moving things to the cloud.[10]

Server virtualization does indeed reduce costs through economies of scale.

Virtualization, however, also opens up a new security risk not typically seen in the traditional IT environment: multitenancy. The "hypervisor," controlled through the application, creates numerous virtual servers, also known as virtual machines (VM). These VMs are each available for "rent" to any customer that requires this service. In a DOD private cloud, all the customers will be DOD entities. In a commercial cloud, the customers could be anyone, including the DOD, the federal government, private citizens, foreign countries, or rogue entities. Discussion of the cloud models will show that the impact multitenancy has on any particular customer will depend on the level of control and the amount of sharing a customer is willing to accept.

While numerous vendors provide hypervisor software capable of creating a VM environment, Bill Kleyman of Data Center Knowledge has identified the "Big Three" hypervisors: VMware vSphere 5, Citrix XenServer 6, and Microsoft Hyper-V.[11] With multiple VMs, multiple applications can run on a single physical server. Numerous organizations and users could use each of the VMs hosted on the physical servers. The Cloud Security Alliance notes that "the lowest common denominator of security will be shared by all tenants in the multitenant virtual environment."[12]

## Infrastructure Models

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, identifies four deployment models for cloud computing: the private cloud, community cloud, public cloud, and hybrid cloud. Each of these models is implemented to allow varying access to the cloud resources.

"*Private cloud*. The cloud infrastructure is provisioned for the exclusive use by a single organization comprising multiple consumers (e.g., business units). 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." A DOD private cloud would be solely owned, operated and managed by the DOD on a DOD premise. This cloud would be used by all DOD components and agencies (business units). "*Community cloud*. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises." A DOD community cloud would also be solely owned, operated, and managed by the DOD on a DOD premise. However, individual DOD components and agencies

(business units) could maintain their own individual "private clouds." "*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. DOD might participate in a public cloud—an external, commercially owned cloud, solely owned, operated, and managed by a commercial organization capable of supporting both government and private entities. "*Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public). They remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). It is through this varying access that the level of accepted security risk is set." DOD might participate in a hybrid cloud—a cloud model composed of two or more clouds of the previously defined models: private, community or public. However, due to security concerns that will be addressed later, interaction between the private and community models will have limited interaction with any pubic portions.[13]

## Cloud Services

There are typically three cloud services: IAAS, PAAS, and SAAS. Together, these build on each other, providing more service to the customer while limiting customers' abilities to operate, maintain, and secure their data and services. The type of cloud service provided ultimately determines the size of an IT department a customer needs. As a customer moves through the cloud services from IAAS to PAAS and finally to SAAS, the IT department shrinks. This also means the customer becomes more reliant on the cloud provider for operational capability and regulatory compliance. This results in cost savings obtained through outsourcing to a public cloud that are balanced against the level of risk a customer is willing to accept. See table 1 in the discussion of SAAS below for a quick comparison of the IT services made available through the various cloud services.

### Infrastructure as a Service

The foundation on which all cloud services are built, IAAS starts the consolidation and virtualization process, developing savings based on economies of scale. The virtualization process mentioned above allows cloud providers to utilize their resources more efficiently. Creating multiple VMs on a single server increases the utilization rate of the server, thus

reducing the number of servers required.[14] This reduction in servers reduces the square footage required to host these servers; heating, ventilation, and air conditioning (HVAC) requirements; electrical costs; and the staff required to maintain equipment and facilities. Savings are created through economies of scale.

However, this is where the customer starts to lose control of the IT infrastructure. The IAAS provider owns the fundamental infrastructure required for a cloud-computing environment. This includes building facilities (data center) and all associated support: physical security, HVAC, electricity, and so on. In addition to the physical environment, the cloud provider also hosts many of the network devices required to control the flow of data to and from the VMs. These devices control the flow of data internal to the cloud, and they become shared resources among all cloud users. They also provide interfaces for users to access the cloud environment. VMs include routers for controlling the flow of data, switches to interconnect the various network devices, firewalls to control the types of data traffic that are allowed in or out, proxy servers for controlling user access to Web pages, and large-scale storage for data management. Each of these devices allows access to the cloud resources and prevents unauthorized access. All of these devices are under control of the cloud provider. Likewise, the provider has a very large role in IT infrastructure security and protection. The customer in an IAAS environment provides operating systems and applications running on VMs. NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, states that "in general, IAAS places more system management responsibility on subscribers than either SAAS or PAAS; subscribers need to manage the VMs and virtualized infrastructure and need to perform system administrator work."[15] Figure 1 shows the division of responsibility with respect to the IT hardware involved. The IAAS provider controls the hardware and hypervisor (defined in the virtualization section), and the user controls the operating systems, middleware, and applications.

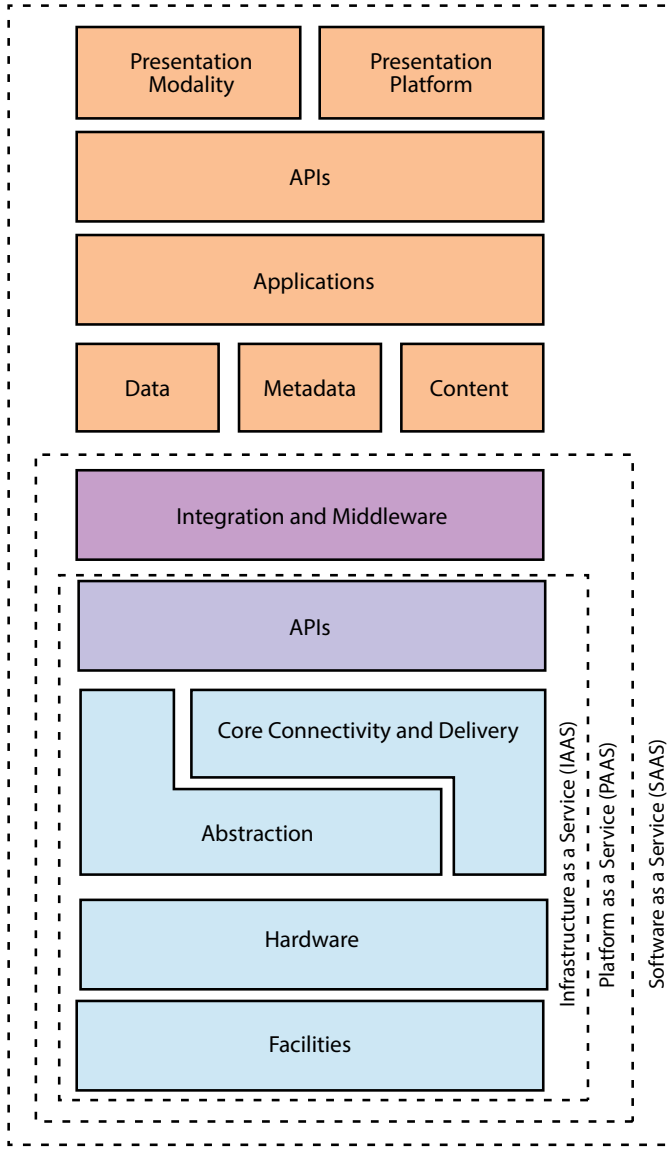



**Figure 1. IAAS component stack and scope of control**. (*Reprinted from* Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas. Special Publication (SP) 800-146, *Draft Cloud Computing Synopsis and Recommendations,* National Institute of Standards and Technology, May 2011.)

## Platform as a Service

PAAS is the next building block in cloud computing. This service has the cloud provider taking on more of the IT functions and further reducing the role the user plays in configuring, managing, and securing IT services and data. In addition to the core service provided by IAAS, PAAS provides a platform for the user to develop applications. Acunetics.com describes Web applications as "computer programs allowing Website visitors to submit and retrieve data to/from a database over the Internet using their preferred Web browser. The data is then presented to the user within their browser as information generated dynamically (in a specific format, e.g. in Hypertext Mark-up Language using Cascading Style Sheets) by the Web application through a Web server."[16] These platforms provided by the PAAS provider may include but are not limited to operating systems such as Windows or Linux, database functions such as Special Query Language or dBase, or Web servers such as Apache or Microsoft Internet Information Server. PAAS ultimately provides services to the user as a Web-based application, with the majority of the processing taking place in the cloud provider's infrastructure. Thus, PAAS applications are very dependent on browser technologies and secure connections to the cloud service provider.[17] However, with PAAS, the end-user organization has the capability to develop, operate, and maintain applications on the cloud provider's infrastructure. Application security rests with the end-user organization while network security rests with the cloud provider. Figure 2 shows the division of responsibility with respect to IT. The PAAS provider controls the hardware, VM software, and the operating system. The user controls only the middleware and applications.

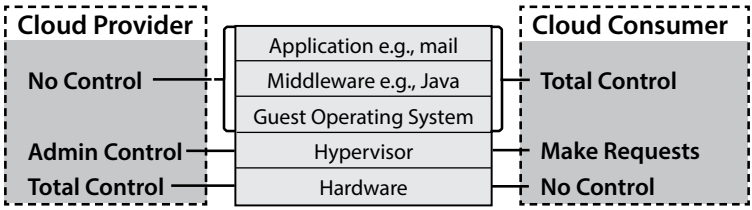



**Figure 2. PAAS component stack and scope of control**. (*Reprinted from* Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas, Special Publication (SP) 800-146, *Draft Cloud Computing Synopsis and Recommendations*, National Institute of Standards and Technology, May 2011.)

**Software as a Service**

The final building block in the cloud service model is SAAS. This model provides maximum service to the user while at the same time taking on most if not all of the security for the user. Just as with PAAS, with SAAS applications, the user's browser is the interface for the application.[18] It is up to the user's organization to ensure that service-level agreements (SLA) or contracts with cloud providers stipulate their operational, maintenance, and security needs. Figure 3 and table 1 show the division of responsibility. The SAAS provider controls the hardware, VM software, operating systems, middleware, and applications. The user only has limited application control.

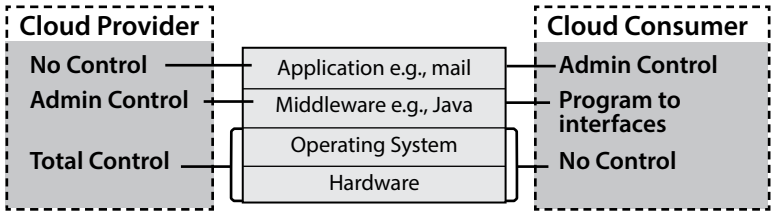



**Figure 3. SAAS component stack and scope of control**. (*Reprinted from* Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas. Special Publication (SP) 800-146, *Draft Cloud Computing Synopsis and Recommendations*, National Institute of Standards and Technology, May 2011.**)**

**Table 1. Cloud service matrix**

| CLOUD | IAAS | PAAS | SAAS |
|---|---|---|---|
| Who are the subscribers? | System administrators | Application developers, application testers, application deployers, application end users | Organizations providing applications to its employees, end users who directly use applications |
| What does the subscriber get? | Virtual computers, network accessible storage, network infrastructure component to include firewalls, configuration services—including networks, servers, and storage | Use of cloud provided tools and execution resources to develop, test, deploy and administer applications. Includes networks, servers, operating systems and storage | Use of specific applications, application data management, data backup and sharing—including networks, servers, operating systems, storage and user applications |

*Reprinted* from Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas. Special Publication (SP) 800-146, *Draft Cloud Computing Synopsis and Recommendations*, National Institute of Standards and Technology, May 2011.

## History of Department of Defense Cloud Computing

The Air Force maintains that "controlling the portions of cyberspace integral to our mission is a fundamental prerequisite to effective operations across the range of military operations."[19] Migration of the DOD's combat support information technology to a cloud infrastructure is not as simple as picking a commercial provider. In fact, numerous directives and public laws control the DOD's and its components' and agencies' abilities to migrate to cloud computing, and many organizations are uncertain how to proceed. A study conducted by Norwich University found that over 43 percent of the federal agencies surveyed were uncertain how they would implement this "cloud first" approach. Over 80 percent indicated that they were either uncertain or did not believe that current federal security standards meet their needs for establishing a cloud infrastructure.[20] Recent and pending legislation like the *Revised Cybersecurity Act of 2012* and the executive order "Improving Critical Infrastructure Cybersecurity" shows a focus on threat information sharing and protecting privacy and civil liberties.[21] All of these hinge on protecting the civilian networks that are critical to the US economy and industrial infrastructure.

While current policy has failed to catch up with the cloud environment, DISA has still managed to make great strides in the deployment of a private DOD cloud. Meanwhile, the commercial clouds leave significant gaps in security and consistency while the identification and certification of providers also lag behind.

### United States Chief Information Officer Directives

According to the *Federal Cloud Computing Strategy* (*FCCS*): "The federal government's current information technology (IT) environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times. These inefficiencies negatively impact the Federal Government's ability to serve the American public." Because of this, the US CIO has called for a cloud first policy recognizing the benefits of cloud technology. Cloud first focuses on the high-level surface benefits of cloud computing—economy, flexibility, and speed—as well as "shift[ing] focuses from asset ownership to service management."[22] The plan also required agencies to perform their initial migration of three internal services to a cloud infrastructure within 18 months.[23]

Unfortunately, the US CIO cloud strategy seems more focused on the cloud as a commercial enterprise than as an internal infrastructure. This is evident in the time frame of 18 months identified for initial migration and in the fact the *FCCS* specifically realizes that "years [are] required to

build data centers for new services."[24] Furthermore, the *FCCS* calls for data center consolidation through the reduction of applications "hosted within government-owned data centers."[25] With this, it is clear that commercial clouds are the desired end state. Indeed, the US CIO directives seem to preclude the development of an internal private cloud that could provide many if not all of the benefits of a commercial cloud.

### *The National Defense Authorization Act of 2012*

The 2012 *NDAA* is consistent with the US CIO direction of cloud first and sets in place requirements for IT transformation. First, the *NDAA* calls for a reduction of IT infrastructure such as square footage of data centers and utility usage (power and HVAC). There are requirements for reductions in investment capital, numbers of applications being utilized, personnel, and the time required to expand IT services using a "just-in-time" service-delivery model and for increasing multiorganization usage.[26] All of these requirements are consistent with the utilization of cloud computing infrastructure, especially for a private DOD cloud environment rather than cloud environments for each component or agency.

However, the *NDAA* also went further by requiring that the DOD CIO develop a plan for the "migration of Defense data and government provided services from department-owned and operated data centers to cloud computing services."[27] Further, there is a call for "utilization of private sector managed security services for data centers and cloud computing services."[28] These requirements do not allow proper evaluation of a DOD cloud that would be capable of providing the same cost savings anticipated through a commercial solution.

### *Department of Defense Cloud Computing Strategy*

Released in July 2012, the *DOD Cloud Computing Strategy* (*DODCCS*) clarifies the DOD's view on the role commercial cloud providers should play within a DOD cloud. Specifically, the *DODCCS* recognizes that cybersecurity within the commercial cloud environment has significantly improved and continues this trend.[29] The launching of the Federal Risk and Authorization Management Program (FEDRAMP) program, which will be discussed later, has made access to precertified commercial vendors even easier for federal agencies. However, the DOD also recognizes that significant risks to the DOD IT infrastructure are present, and migration to commercial cloud environments increases these risks.[30] Even with this realization, the *DODCCS* still pushes forward with the migration of

DOD data to commercial cloud infrastructures. The DOD is looking to "leverage externally provided cloud services, i.e., commercial services, to expand cloud offerings beyond those offered within the Department" while continuing to develop the internal DOD core cloud services.[31] Furthermore, the DOD wants to migrate its IT system with low or moderate risk levels to commercial cloud infrastructure. These risk levels will be covered later with cloud standards and IT regulations. The *NDAA* and the *DODCCS* push forward with commercialization without first establishing a robust private cloud and then evaluating the need and cost effectiveness of commercialization.

## Data Security Regulations/Standards

Moving from a traditional client/server configuration to a cloud-computing configuration does not relieve the federal departments and agencies from meeting regulatory requirements to protect federal IT systems and the data they store. These identify responsibilities and set the security standards. However, many of these requirements were written prior to the establishment of cloud computing environments and, therefore, do not address the risks associated with cloud computing. Still, others provide only very high-level guidance with respect to the cloud environment and leave the individual components and agencies to set actual security standards.

### *The E-Government Act of 2002*

Enacted in December 2002, Public Law 107-347 establishes "a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes."[32] Subchapter 3, "Information Security," provides "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets."[33] This framework is known as the *Federal Information Security Management Act of 2002* (*FISMA*). The *FISMA* requires identifying standards for cloud computing:

- the establishment of the criteria for measuring information security and
- the establishment of the NIST as the organization responsible for setting security standards for federal information system.

The *FISMA* identifies three security objectives for securing information systems:

> Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
>
> Integrity: Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and
>
> Availability: Ensuring timely and reliable access to and use of information.[34]

While each of these security objectives is critical to the security of the underlying IT infrastructure of the cloud, they are not necessary considerations in a cloud-computing environment. A quick look at each area will help identify the specific areas that must be considered in a cloud environment.

The DOD implementation of public key infrastructure (PKI) has been addressed the first two areas, confidentiality and integrity. The DISA states that PKI provides identification and authentication, data integrity, confidentiality, and technical nonrepudiation.[35] PKI provides integrity by applying a "digital signature" that the identifies of the data source and confirms that the information has not been tampered with. Encryption of the data provides confidentiality. This is where a cloud environment can start to fall short of meeting the security requirements. As stated earlier, PAAS and SAAS are mostly Web-based applications, with the PKI encryption between the user and the Web application. Depending on the access level the provider has to the cloud service, this potentially could give the cloud provider unauthorized access to data.

Perhaps the biggest issue with respect to the cloud environment is availability. Cloud services previously identified are IAAS, PAAS, and SAAS. With the successive application of each, cloud service providers take on more responsibility for providing the IT infrastructure and take away user control. While contractual requirements in SLA may specify "reliability rates," the owner of the cloud controls the user's ability to access and use data and services.

**The National Institute of Standards and Technology**

The NIST is identified in the *FISMA* as the organization responsible for the development of standards related to the security of IT systems, and it produces numerous publications about securing IT systems. These include special publications and Federal Information Processing Standards publications (FIPS pub).The cornerstone for identifying the standard, FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, lays out the process for categorizing the likely effects of data or systems compromises on an organization. These security categories are defined in terms of an IT system's ability to achieve the *FISMA* security objectives of confidentiality, integrity, and availability. Each security objective is given a risk value of low, moderate, or high. An objective is at low risk if compromise could result in "limited adverse effects." Moderate risks could result in "serious adverse effects," and high risks could result in "severe or catastrophic adverse effects." Taken directly from FIPS PUB 199, table 2 shows the criteria used to categorize the IT systems and data.

Applying the criteria in table 2, the evaluator will come up with a security category (SC), using the format below for each IT systems and data types using the formula "SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}."[36]

Once a system has been categorized, FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, and SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, are used to identify the appropriate security measures for protection of the systems and data.[37] Consistent security categorization is missing across the federal government and especially in the DOD. NIST SP 800-60 attempts to refine this process by first separating the data/systems into four business categories—service for citizens, mode of delivery, support delivery of services, and management of government resources.[38] The SP then provides recommendations for each category.

These are recommendations, and system owners have the ultimate authority to set each category. Furthermore, these recommendations were written before there was a requirement to utilize cloud technology. These categorizations do not consider that IT systems and data may end up in a public cloud, exposed to the higher security risks associated with those environments. Finally, military operations are not specifically identified and, therefore, are referred to best-fit business categories. The DOD is left on its own.

**Table 2. Potential impact definitions for security objectives**

| POTENTIAL IMPACT | | | |
|---|---|---|---|
| Security Objective | LOW | MODERATE | HIGH |
| ***Confidentiality*** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| ***Integrity*** Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. [44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| ***Availability*** Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

*Reprinted from* FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004.

### Department of Defense Instructions

The categorization process described in the previous section is not new. However, the public sector has not had to deal with the categorization process. Public cloud infrastructure used for DOD purposes would be a DOD IT infrastructure that is subject to *FISMA* certification and accreditation processes. According to DODI 8510.01, *DOD Information Assurance Certification and Accreditation Process* (*DIACAP*), the responsibility for meeting *FISMA* requirements is at the component and agency level.[39] Once again, this delegation of categorization responsibility does not allow for standardization of the process and, therefore, is not clear DOD guidance for migration to commercial cloud infrastructure.

Another arena where the DOD departs from the practices of other federal agencies and the IT industry is in the area of operations security (OPSEC). DODD 5205.02E, *DOD Operations Security Program*, defines the OPSEC process as identifying and protecting pieces of information that when put together may have value to an adversary, thus presenting an unacceptable risk.[40] The *Washington Post* printed an OPSEC anecdote where a Domino's Pizza franchise owner claimed he could predict significant events based on an increase in pizza deliveries in the Washington, DC, area.[41] The accuracy of the story is debated, but a simple piece of information can lead to information of value to our enemies. Likewise, the owner of a cloud environment has access to the server utilization rates. While the cloud owner may not have access to the actual data, it would be possible to tell when activity has increased, perhaps an indicator of near future DOD activity and a clear OPSEC risk.

## Current Program Evaluations

The US CIO's December 2010 call for migration to cloud computing required each federal agency to identify three services for migration to the cloud and to have that migration complete within 18 months.[42] Twenty-six months later, the DOD strategy on cloud computing was only six months old, and the military components and other federal agencies were building their own, independent paths toward cloud computing. Furthermore, the federal structure to provide commercial cloud infrastructure, FEDRAMP, has significant shortcomings with respect to support for DOD cloud requirements.

### Department of Defense Cloud Programs Evaluated

The failure of the DOD to implement a cohesive cloud computing strategy has allowed the Army, Navy, Air Force, and DISA to take diverging

paths and fail to maximize economies of scale. Compounding these failures in economies of scale, each of the military components of the DOD has migrated specific systems to commercial clouds without considering the consequences to its own IT infrastructures.

**The Navy**. The Department of the Navy (DON) is currently migrating from the existing Navy–Marine Corps Intranet (NMCI) to the new Next Generation Enterprise Network (NGEN). This plan highlights many of the failures of the DOD to manage cloud computing and highlights one of the increased security risks associated with commercial IT infrastructure, including commercial clouds.

First, the DON published the NGEN: network operations concept of operations (CONOPS) in April 2008. This CONOPS is a USN/USMC-centered plan for a government-owned, contractor-operated infrastructure without any mention of cloud concepts or services.[43] As such, this plan fails to take advantage of the economies of scale. In fact, the Government Accountability Office (GAO) in a 2012 report found "DON has not yet shown that it is pursuing the most cost-effective approach for acquiring NGEN capabilities."[44]

Finally, this transition from NMCI to NGEN highlights a serious security risk associated with contracted service, availability. This is one of the three security factors addressed in the *FISMA* standards. The same GAO report indicated that the DON had to award a $3.4 billion contract to bridge the gap between the end of the NMCI contract and transition to the NGEN infrastructure.[45] Had this negotiation failed, the DON would have faced a network and mission failure.

**The Air Force**. The goal of the Air Force Network (AFNET) program is to create one enterprise network for the Air Force through the consolidation of over 400 base networks.[46] However, while the Air Force is claiming one enterprise network, it also recognizes that it "will not try to make AFNET all things to all people."[47] Even as this transformation progresses, key end users such as Air Combat Command (ACC) are struggling to understand what the "enterprise" is. Brig Gen David Uhrich, ACC director of communications, was quoted as saying, "The first thing I'd like to know is what the heck is the enterprise? Has anybody seen a definition of the core services the enterprise will provide?"[48] Maj Gen Suzanne Vautrinot, commander, Air Force Cyber Command stated, "Getting the entire military onto something that resembles one network is going to be a costly and slow process."[49] Indeed, the Air Force is transforming and has downplayed efforts to develop a DOD cloud transformation solution.

**The Army's Information Systems Agency**. The Army is perhaps the success story. Its migration to cloud service has taken two approaches in line with the 2012 *NDAA*. First, a commercial cloud provider was utilized,

Salesforce.com, for the Army Recruiting Information Support Systems (ARISS). This program proved invaluable to the Army, converting an estimated $1 million infrastructure procurement to a $54,000/year commercial contract. This new system resulted in "faster application upgrades, dramatically reduced hardware and IT staff costs, and significantly increased staff productivity."[50] However, availability of this system is still dependent on successful contract negotiations and fulfillment. This is only one of the Army's IT systems. Transforming a single system does not take advantage of the capacities of existing systems and the economies of scale that would be available with an Army private cloud.

**The Defense Information Systems Agency**

DISA is leading the way for the development of a private DOD cloud computing environment in conjunction with the Army. Operational in 2008, DISA implemented its Rapid Access Computing Environment (RACE) as an IAAS capability available to all DOD components and agencies. Specifically, the RACE is a "self-service provisioning Web portal, allowing DOD users to provision servers within a secure computing environment."[51] The Army has capitalized on these DISA service capabilities by migrating e-mail services to the DISA-provided capability. To date, over 500,000 e-mail users are on the DISA-provided service. The Army anticipates this will save over $380 million through fiscal year 2017.[52]

**Federal Commercial Cloud Service Initiative**

Established to precertify commercial cloud providers, the FEDRAMP has large gaps in its ability to provide commercial cloud providers that meet DOD demands. The following are the purposes of the FEDRAMP:

- ensure that cloud-based services used government-wide have adequate information security,
- eliminate duplication of effort and reduce risk-management costs, and
- enable rapid and cost-effective procurement of information systems / services for federal agencies.[53]

The following are the goals of the FEDRAMP:

- accelerating the adoption of secure-cloud solutions through reuse of assessments and authorizations,
- increasing confidence in the security of cloud solutions,

- achieving consistent security authorizations using a baseline set of agreed-upon standards and accredited independent third-party assessment organizations,
- ensuring consistent application of existing security practices,
- increasing confidence in security assessments, and
- increasing automation and near real-time data for continuous monitoring.[54]

Despite these purposes and goals, FEDRAMP is not capable of meeting the stringent demands of DOD security. The FEDRAMP CONOPS specifically states, "FEDRAMP defines a set of controls for low and moderate impact level systems."[55] Indeed, the FEDRAMP program cannot be a complete solution. It only provides certification for two of the three levels of certification.

Finally, two of the biggest concerns with commercial clouds are geolocation of data and multitenancy on the hardware. Geolocation refers to knowing the exact physical location of the data. With a commercial cloud, DOD data could be located on any physical server within the providers' clouds. This location could include countries with different laws on privacy of data than those of the United States and could include countries hostile to the United States. In an article written for the Naval Postgraduate School on data sovereignty, the authors point out that verifying where one's data is physically located is a critical issue.[56]

Multitenancy refers to data or services of different customers residing on the same physical hardware. This is where commercial cloud providers make their money through economies of scale.[57] Just as with geolocation of data, this could result in US data being physically located in countries or with that of parties hostile to the United States. Rob Carey, deputy DOD CIO, found this to be a significant security risk in utilizing commercial infrastructure.[58] Unfortunately, FEDRAMP does not address this.. Instead, individual users must address this critical issue of security in SLAs.[59]

## Comparison of Alternatives

Cloud computing, its associated risks and benefits, and the fact that DOD military components and agencies have to develop individual cloud strategies were previously explained. Unfortunately, this DOD hands-off approach is flawed. Intended to "address use of commercial cloud services in the Department's multiprovider enterprise cloud environment," the approach fails to capitalize on the economies of scale that

are possible.[60] This approach has allowed the military components and agencies to maintain redundant systems and contract with several commercial cloud providers. There are three potential cloud models for the DOD to consider implementing: public solution, private solution, and a hybrid solution.

**The Public Solution**

The National Security Agency (NSA) identified increased security risks as the greatest issue with public clouds: "Due to this issue of the movement of the trust boundary, public clouds (whereby cloud resources are dynamically provisioned over the Internet) represent the greatest challenge from a security perspective."[61] The *DODCCS* and FEDRAMP both recognized the risks associated with public clouds in their common policy of not utilizing commercial providers for any systems above a moderate security classification. Jon Toigo of Informationweek.com notes that SLAs that ensure security beyond the moderate level, force cloud providers to violate their economies of scale and reduce the cost benefits to the customer.[62] Moving DOD data and services to commercial clouds presents a much larger level of risk. Rob Carey, deputy DOD CIO, points out that one of the significant security risks to utilizing commercial infrastructure is "multitenancy" that is inherent in commercial cloud infrastructures.[63] Furthermore, with data on a commercial cloud potentially residing anywhere in the world, the sovereignty of DOD data could be in jeopardy. Vivek Kundra, federal CIO, states that this is a matter of international law which is still to be addressed and resolved.[64] Some argue that commercial providers have made significant progress in securing their networks to meet DOD requirements. However, the General Services Administration has yet to list any *FISMA*-certified commercial SAAS vendors on the Info.apps.gov Website. IAAS vendors are also not certified to provide service across all *FISMA* categories of security. This means that commercial vendors cannot fully support the DOD requirements.[65] With an estimated 75–95 percent excess capacity within the typical DOD IT enterprise, enormous cost savings are available in the consolidation of DOD IT infrastructure before even considering a move to commercial clouds. Given the increased security risks or decreased economies of scale, a public cloud does not present a valid option.

**The Private Solution**

The cloud-computing concept could yield positive financial results. However, smaller companies employing private clouds do not realize these kinds of results. Only extremely large data centers can provide true

economies of scale through cloud computing.[66] With over 772 data centers across the DOD, the whole organization, not the individual components and agencies, is clearly an extremely large IT enterprise.[67] The whole DOD would be capable of achieving very large economies of scale.

Locating all infrastructure in the "internal data centers" of a private cloud diminishes many of the security risks. Geolocation and data sovereignty cease to be issues. All data facilities within a private cloud would be DOD facilities located on DOD property. This makes the systems and data subject to US law. As for multitenancy, users of the DOD private cloud would be limited to the DOD components and agencies.

There are significant disadvantages to this solution. It does not meet the *NDAA* requirement to utilize commercial resources, and it does not make cloud computing a hands-off endeavor from a DOD perspective. The first issue will be dealt with subsequently. This solution takes responsibility for managing hardware and software off the components and agencies and consolidates it at the DOD level. From the component and agency perspective, the cloud is a hands-off solution.

### The Hybrid Solution

The last model is the hybrid model, which best identifies the current structure of DOD cloud computing. This model could meet the *NDAA* mandate to use commercial providers. As previously noted, however, commercial economies of scale present higher security risks to the systems and data. With the security requirements left to the individual component or agency, there is no clear, overall, standard guidance on security classification. Therefore identifying data/services that should migrate to the commercial portion of the hybrid cloud is complex. Since the components and agencies are to identify the data/services for migration and SLA through the FEDRAMP process, the DOD misses economies of scale in the contract arena. Multiple contracts could potentially be combined for better pricing. Migrating data/services to the commercial cloud prior to building the private DOD cloud may miss the economies of scale still available to host those services on a private cloud.

## Recommendations

The US CIO directives, the *NDAA*, and the *DODCCS* all call for the use of commercial cloud infrastructure as a part of the DOD cloud migration. These directives call for parallel paths with commercial and private cloud development occurring simultaneously. Tari Takai, DOD CIO, said, "We don't want to see an ad hoc move to the cloud; we want to see a

DOD-wide perspective."[68] Even with this, the *DODCCS* allows for the potential use of multiple commercial vendors and numerous individual component and agency cloud solutions. This is completely contrary to the concept of "a DOD-wide perspective." There may very well be data that can safely be placed on a commercial cloud. However, until the DOD private cloud is fully implemented, a migration to a commercial cloud would be a move into uncharted territory and ill-advised.

The following proposals are made to migrate the DOD to a cloud environment, ensuring risk mitigation and maximum economies of scale while heading down a path that ultimately allows for a potential hybrid solution.

**Perform Security Category Revaluation of Systems and Data**

First, decide what data and services ought to move to a commercial cloud. The DOD needs to evaluate its directions provided in *DIACAP*. The process needs to be standardized across all components and agencies to ensure that all similar data and services are given the same security classification. This process also needs to develop a set of sensitivity levels and protection requirements for unclassified data for commercial cloud migration. This means determining the data and services that can be placed on commercial cloud services without risks associated with geolocation, multitenancy, data sovereignty, and availability. These standards of evaluation should then be used throughout the remaining processes.

**Move All Noncommercial Data and Services to a Private Cloud**

The next step should be to implement a private DOD cloud that maximizes the available economies of scale while applying the required level of security needed. This should happen before migrating any data/services to the commercial cloud. The DISA, with an existing cloud environment, including the RACE and DOD Enterprise Email, should be mandated to build the DOD private cloud infrastructure. All DOD components and agencies should be required to migrate to the DISA private cloud infrastructure. This ought to be done to reduce significantly or eliminate the security risks associated with cloud computing. In addition, the size of the DOD IT infrastructure should enable the maximum economies of scale through cloud computing.

**Perform Cost Analysis on Where To Host Low-Security Classification Services**

Once data and services that cannot be hosted in a commercial cloud are secured within the private DOD cloud, a detailed cost analysis of hosting "commercial-ready" data and services on the existing private cloud versus hosting on a FEDRAMP-approved commercial cloud should be conducted. This analysis should be done at the DOD level and not at the individual component and agency level. More importantly, it should not be done at the individual program level as is the current practice. The migration should take place if it is more cost-effective and there are no data/system protection issues—geolocation, multitenancy, data sovereignty, and availability. However, if cost savings cannot be found to be more cost-effective, the DOD should engage Congress to reevaluate the requirements set forth in the 2012 *NDAA*.

## Conclusion

The DOD transformation to cloud computing is off to a rather poor start. This is exactly the sort of start that Tari Takai was hoping to avoid as the DOD attempts to develop a "standardized approach to cloud computing adoption."[69] To date, the transformation lacks a focus that permits the DOD to achieve economies of scale and does not ensure adequate protections for the IT systems and data.

The US CIO's *25 Point Implementation Plan to Reform Federal Information Technology Management*, his 2011 *Federal Cloud Computing Strategy*, and the congressional mandate in the *NDAA* have set forth a path to cloud transformation that is focused on commercial cloud providers. Facing the requirement to complete a first migration to the cloud in 18 months, the DOD left it to the components and agencies to find individual solutions to meet this requirement. It was 20 months after the US CIO directive before the release of the *DODCCS* providing initial uniform guidance for the components and agencies to follow.

Outdated policy and regulations do not specifically address the new and increased risks associated with cloud computing: geolocation, data sovereignty, multitenancy, and availability. These new and existing risks are much more severe in a commercial cloud environment. Current guidelines are vague and leave to the individual components and agencies to categorize the security level of IT systems and to identify the systems and data appropriate for the elevated risks associated with commercial cloud computing environments. The NSA and DOD CIO have both publicly

recognized that placing IT systems and data in a commercial cloud environment put these systems and data at an elevated risk.

The options available to the DOD for cloud transformation each have their benefits and associated risks. Placing the entire DOD cloud infrastructure on a commercial cloud is clearly not an option. The security risks associated with a commercial cloud are too high and attempting to mitigate or eliminate the risks would eliminate the savings achieved through economies of scale.

The development of a DOD private cloud provides the best option to achieve savings through economies of scale while still providing the required level of protection needed to secure DOD systems and data, including providing OPSEC. Unfortunately, there are still the US CIO and *NDAA* requirements to utilize commercial cloud providers.

The third option of using both commercial and private cloud infrastructure (hybrid) provides the best chance to meet regulatorily as well as risk mitigation requirements. However, until a DOD private cloud has been implemented, the cost savings available through partial commercialization cannot be identified.

It is not too late to develop a DOD strategy that ensures protection of the DOD IT systems and at the same time takes advantage of the economies of scale available at the DOD level. First, the DOD should standardize system for categorizing the protection levels assigned to its data and systems. Second, the DOD should develop and mandate the use of a private DOD cloud. Then the DOD should evaluate the potential cost savings associated with using commercial cloud providers with the least risk to data and systems. These steps will allow the DOD to harness the power of cloud computing while balancing an acceptable risk at an acceptable cost.

**Notes**

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Corrin, "Budget Struggles."
2. Kundra, *25 Point Implementation Plan*.
3. *National Defense Authorization Act* (*NDAA*), 707.
4. Mell and Grance, Special Publication (SP) 800-145, *National Institute of Standards and Technology Definition of Cloud Computing*, 2.
5. Waters, "Virtualization Definition and Solutions."
6. Hindle, "Economies of Scale."
7. "What Is Cloud Computing," Salesforce.com.
8. Serbu, "DISA [Defense Information Systems Agency] Pushes Efficiency."
9. Yager, "Reality of Virtual Servers."
10. Marshall, "Top 10 Benefits of Server Virtualization."

11. Kleyman, "Hypervisor 101."
12. "Security Guidance," 159.
13. Mell and Grance, "SP 800-145, *NIST Definition of Cloud Computing*, 3.
14. Yager, "Reality of Virtual Servers."
15. Badger et al., SP 800-146, *Draft Cloud Computing Synopsis*, 7-5.
16. "Web Applications," Acunetix.com.
17. Ibid., 6-4.
18. Ibid., 5-1.
19. Air Force Doctrine Document 3-12, *Cyberspace Operations*, ii.
20. Perera, "Federal Agencies Uncertain How to Respond."
21. "Featured Legislation," US Senate Committee; and Obama, "Executive Order—Improving Critical Infrastructure Cybersecurity."
22. Kundra, *Federal Cloud Computing Strategy*, 1–3.
23. Ibid., 3; and Kundra, *25 Point Implementation Plan*, 7.
24. Kundra, *Federal Cloud Computing Strategy*, 3.
25. Ibid., 8.
26. *NDAA*, 703-7.
27. Takai, "DOD Cloud Computing Strategy," 3.
28. *NDAA*, 706.
29. Takai, "DOD Cloud Computing Strategy," 24.
30. Ibid., 24.
31. Ibid., E-3 and 10.
32. *E-Government Act*, 2899.
33. Ibid., 2946.
34. Stine et al., SP 800-60, *Guide for Mapping*, 9.
35. "About PKI and PKE," DISA.
36. Federal Information Processing Standards Publication (FIPS Pub) 199, *Standards for Security Categorization*, 5.
37. FIPS Pub 200, *Minimum Security Requirements*; Joint Task Force, SP 800-53, *Security and Privacy Controls*; and Stine et al., *Guide for Mapping*, 12.
38. Stine et al., *Guide for Mapping*, 14.
39. Department of Defense Instruction 8510.01, *Information Assurance Certification*, 7.
40. Department of Defense Directive 5205.02E, *DOD Operations Security Program*, 11.
41. Schaffer, "With Capital in Panic."
42. Kundra, *25 Point Implementation Plan*, 7.
43. Government Accountability Office 12-956, *Next Generation Enterprise Network*, 11.
44. Ibid., 13.
45. Ibid., 3.
46. Serbu, "Air Force Aims for One Network."
47. Ibid.
48. Ibid.
49. Serbu, "Cyber Command Boss Wants Better Integration."
50. Kundra, "State of Public Sector Cloud Computing," 12.

51. Slabodkin, "DISA Outlines Major Network and Enterprise Initiatives."

52. DISA, "DISA and Army Achieve DOD Enterprise Email Milestone."

53. Government Services Administration (GSA), "Federal Risk and Authorization Management Program Concept of Operations," 10.

54. GSA, "FEDRAMP [Federal Risk and Authorization Management] FAQ."

55. GSA "Federal Risk and Authorization Management Program Concept of Operation," 24.

56. Peterson, Gondree, and Beverly, "Position Paper on Data Sovereignty," 1.

57. Kwock, "Multi-Customer, Multi-Tenancy Considerations."

58. Corrin, "Budget Struggles, Cyber Policies Shape DOD Approach to Cloud."

59. "Federal Risk and Authorization Management Program Control-Specific Contract Clauses," Cloud.Cio.gov, 1.

60. Takai, "DOD Cloud Computing Strategy," Forward.

61. *Cloud Computing—Overview of Information Assurance Concerns and Opportunities Version 1.02*, NSA.gov, 2.

62. Toigo, "Evaluating Storage-as-a-Service."

63. Corrin, "Budget Struggles."

64. Walker, "Kundra: Cloud Computing Data Sovereignty a Matter for 'International Law.'"

65. GSA, "Apps.gov Cloud FAQs."

66. Armbrust et al., "A View of Cloud Computing," 52.

67. Moloney Figliola, Andrews, and Fischer, *Department of Defense Implementation of the Federal Data Center*, 11.

68. Walker, "Takai: DOD-Wide Cloud Strategy Taking Shape."

69. Ibid.

# Abbreviations

| | |
|---|---|
| ACC | Air Combat Command |
| AFNET | Air Force Network |
| ARISS | Army Recruiting Information Support Systems |
| CIO | chief information officer |
| CONOPS | concept of operations |
| *DIACAP* | *DOD Information Assurance Certification and Accreditation Process* |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| *DODCCS* | *DOD Cloud Computing Strategy* |
| DON | Department of the Navy |
| *FCCS* | *Federal Cloud Computing Strategy* |
| FEDRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standards |
| FIPS Pub | FIPS publication |
| *FISMA* | *Federal Information Security Management Act of 2002* |
| GAO | Government Accountability Office |
| HVAC | heating, ventilation, and air conditioning |
| IAAS | information as a service |
| IT | information technology |
| *NDAA* | *National Defense Authorization Act* |
| NGEN | Next Generation Enterprise Network |
| NIST | National Institute of Standards and Technology |
| NIST SP | NIST special publication |
| NMCI | Navy–Marine Corps Intranet |
| NSA | National Security Agency |
| OPSEC | operations security |
| PAAS | platform as a service |
| PKI | public key infrastructure |
| RACE | Rapid Access Computing Environment |
| SAAS | software as a service |
| SC | security category |
| SLA | service-level agreements |
| USA | Army |
| USAF | Air Force |
| USMC | Marine Corps |
| USN | Navy |
| VM | virtual machine |

# Bibliography

"About PKI and PKE." Defense Information Systems Agency (DISA). http://iase.disa.mil/pki-pke/Pages/about.aspx.

Air Force Doctrine Document 3-12. *Cyberspace Operations*, 30 November 2011.

Armbrust, Michael, et al. "A View of Cloud Computing." *Communications of the ACM* 53, no.4 (April 2010): 50–58.

Badger, Lee, Tim Grance, Robert Patt-Corner, and Jeff Voas. Special Publication (SP) 800-146. *Draft Cloud Computing Synopsis and Recommendations*. National Institute of Standards and Technology (NIST), May 2011. http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.

Chow, Richard, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control." In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, Chicago, Illinois, November 2009. New York: ACM, 2009. https://www.parc.com/content/attachments/Controlling-DataInTheCloud-CCSW-09.pdf.

*Cloud Computing—Overview of Information Assurance Concerns and Opportunities Version 1.02*. NSA.gov, 18 December 2009. https://www.nsa.gov/ia/_files/support/Cloud_Computing_Guidance.pdf.

Corrin, Amber. "Budget Struggles, Cyber Policies Shape DOD Approach to Cloud." DefenseSystems.com, September 2011. http://defensesystems.com/articles/2011/09/07/ds-summit-rob-carey-Cloud-computing.aspx.

Defense Information Systems Agency (DISA). "DISA and Army Achieve DOD Enterprise Email Milestone." News and Events, 2012. http://www.disa.mil/News/PressResources/2012/dee500.

Department of Defense Directive 5205.02E. *DOD Operations Security Program*, 20 June 2012. http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf.

Department of Defense Instruction (DODI) 8500.2. *Information Assurance Implementation*, 6 February 2003.

DODI 8510.01. *Information Assurance Certification and Accreditation Process*, 29 November 2007.

*The E-Government Act of 2002*. Public Law 107-347, 107th Congress, 17 December 2002. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

*Featured Legislation: The Revised Cybersecurity Act of 2012*. US Senate Committee on Commerce, Science and Transportation, 20 July 2012. http://commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord_id=0cf54f6c-afda-4431-886f-12c632b60daf.

Federal Information Processing Standards Publication (FIPS Pub) 199. *Standards for Security Categorization of Federal Information and Information Systems*. NIST, February 2004.

———. 200. *Minimum Security Requirements for Federal Information and Information Systems*. NIST, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

"Federal Risk and Authorization Management Program [FEDRAMP] Control-Specific Contract Clauses." Cloud.Cio.gov, 4 June 2012. https://cloud.cio.gov/sites/default/files/documents/files/FedRAMP%20Control%20Specific%20Contract%20Clauses%20v2.0.docx.

General Services Administration (GSA). "Apps.gov Cloud FAQs." https://www.apps.gov/Cloud/information/page.do?&keyName=CLOUD_FAQ.

———. "Federal Risk and Authorization Management Program Concept of Operations," 4 June 2012. http://www.gsa.gov/graphics/staffoffices/CONOPS_V1.1_07162012_508.pdf.

———. "FEDRAMP FAQ." GSA.gov. http://www.gsa.gov/portal/category/102439.

Government Accountability Office (GAO) 12-956. *Next Generation Enterprise Network: Navy Implementing Revised Approach, but Improvement Needed in Mitigating Risks*. GAO, September 2012.

Hindle, Tim. "Economies of Scale." *The Economist*, 20 October 2008. http://www.economist.com/node/12446567.

Jansen, Wayne, and Timothy Grance. SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*. NIST, January 2011.

Joint Task Force, Transformation Initiative. SP 800-53, Rev 3. *Recommended Security Controls for Federal Information Systems and Organizations*. NIST, May 2010. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

———. SP 800-53, Rev. 4. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Kajeepeta, Sreedhar. "Multi-Tenancy in the Cloud: Why It Matters," CIO.com, April 12, 2010. http://www.cio.com/article/590731/Multi_Tenancy_in_the_Cloud_Why_it_Matters ?page=1&taxonomyId=3024.

Kleyman, Bill. "Hypervisor 101: Understanding the Virtualization Market." DataCenterKnowledge.com, 1 August 2012. http://www.datacenterknowledge.com/archives/2012/08/01/hypervisor-101-a-look-hypervisor-market/.

Kundra, Vivek. *Federal Cloud Computing Strategy*. The White House, 8 February 2011. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.

———. "State of Public Sector Cloud Computing." Office of Electronic Government, 20 May 2010. https://cio.gov/wp-content/uploads/downloads/2012/09/StateOfCloudComputingReport-FINAL.pdf.

———. *25 Point Implementation Plan to Reform Federal Information Technology Management*. The White House, 9 December 2010. https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

Kwashnik, Gretchen. "Negotiating Contract for Cloud-Based Software." Department of the Navy Chief Information Officer, 17 January 2012. http://www.doncio.navy.mil/ContentView.aspx?id=3585.

Kwock, David. "Multi-Customer, Multi-Tenancy Considerations." Thoughts on Cloud.com, 29 July 2011. http://thoughtsoncloud.com/index.php/2011/07/multi-customer-multi-tenancy-considerations/.

Marshall, David. "Top 10 Benefits of Server Virtualization." *Infoworld.com*, 2 November 2011. http://www.infoworld.com/d/virtualization/top-10-benefits-server-virtualization-177828.

Mell, Peter, and Timothy Grance. NIST SP 800-145. *The NIST Definition of Cloud Computing*. NIST, September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Moloney Figliola, Patricia, Anthony Andrews, and Eric A. Fischer. *Department of Defense Implementation of the Federal Data Center Consolidation Initiative: Implications for Federal Information Technology Reform Management*. Congressional Research Service, 12 July 2012. http://fas.org/sgp/crs/natsec/R42604.pdf.

*The National Defense Authorization Act for Fiscal Year 2012*. S.1867, 112th Congress 1st Session. http://www.gpo.gov/fdsys/pkg/BILLS-112s1867es/pdf/BILLS-112s1867es.pdf.

*Next Generation Enterprise Network: Network Operations Concept of Operations.* Public.Navy.mil, 7 April 2008. http://www.public.navy.mil/spawar/PEOEIS/NEN/NGEN/Documents/NGEN%20NetOps%20CONOPS%20v1[1].0%20Final_rel.pdf.

Obama, Barack. "Executive Order—Improving Critical Infrastructure Cybersecurity." The White House, 12 February 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Perera, David. "Federal Agencies Uncertain How to Respond to 'Cloud First.'" FierceGovernementIT.com, 23 May 2011. http://www.fiercegovernmentit.com/story/federal-agencies-uncertain-how-respond-Cloud-first/2011-05-23.

Peterson, Zachary N. J., Mark Gondree, and Robert Beverly. "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud." In *Proceedings of the USENIX Workshop on Hot Topics in Cloud Computing* (HotCloud), 2011. http://znjp.com/papers/peterson-hotcloud11.pdf.

"Rapid Access Computing Environment." DISA. http://www.disa.mil/Services/Enterprise-Services/Infrastructure/RACE.

Robinson, Neil, Lorenzo Valeri, Jonathan Cave, Tony G. Thompson-Starkey, Hans Graux, Sadie Creese, and Paul Hopkins. *The Cloud: Understanding the Security, Privacy and Trust Challenges*. Santa Monica, CA: RAND, 2011. http://www.rand.org/pubs/technical_reports/TR933.html.

Schaffer, Sarah. "With Capital in Panic, Pizza Deliveries Soar." *Washington Post*, 18 December 1998. http://www.washingtonpost.com/wp- srv/politics/special/clinton/stories/pizza121998.htm.

"Security Guidance for Critical Areas of Focus in Cloud Computing V3.0." CloudSecurityAlliance.org, 2011. https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf.

Serbu, Jared. "Air Force Aims for One Network by End of 2012." FederalNewsRadio.com, 31 October 2011. http://www.federalnewsradio.com/395/2613793/Air-Force-aims-for-one-network-by-end-of-2012.

———. "Cyber Command Boss Wants Better Integration of Network Warriors." FederalNewsRadio.com, 24 August 2012. http://www.federalnewsradio.com/474/3006078/CyberCommand-boss-wants-better-integration-of-network-warriors.

———. "DISA Pushes Efficiency, Security Virtues of DOD Private Cloud." FederalNewsRadio.com, 18 January 2012. http://www.federalnewsradio.com/241/2710869/DISA-pushes-efficiency-security-virtues-of-DoD-private-cloud.

Slabodkin, Greg. "DISA Outlines Major Network and Enterprise Initiatives." DefenseSystems.com, 1 April 2011. http://defensesystems.com/Articles/2011/03/29/Cover-Story-DISA-charts-cloud-strategy.aspx?Page=1.

Stine, Kevin, Rich Kissel, William C. Barker, Jim Fahlsing, and Jessica Gulick. SP 800-60, vol. 1, rev. 1. *Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST, August 2008.

———. SP 800-60, vol. 2, rev. 1. *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.* NIST, August 2008.

*Strategic Plan 2013-2018 Version 1.* DISA, September 2012.

Takai, Teresa M. "Department of Defense Cloud Computing Strategy." Department of Defense, July 2012. http://www.defense.gov/news/DoD CloudComputingStrategy.pdf.

Toigo, Jon W. "Evaluating Storage-as-a-Service," InformationWeek.com, 9 May 2009. http://www.informationweek.com/services/storage /evaluating-storage-as-a-service-options/217300686.

Walker, Molly. "Kundra: Cloud Computing Data Sovereignty a Matter for 'International Law.'" FierceGovernmentIT.com, April 2011. http://www .fiercegovernmentit.com/story/kundra-Cloud-computing-data-sover eignty-matter-international-law/2011-04-10.

———. "Takai: DOD-Wide Cloud Strategy Taking Shape." FierceGovern mentIT.com, May 2011. http://www.fiercegovernmentit.com/story /takai-dod-wide-cloud-strategy-taking-shape/2011-05-25.

Waters, John K. "Virtualization Definition and Solutions." CIO.com, 15 March 2007. http://www.cio.com/article/40701/Virtualization_Defi nition_and_Solutions.

"Web Applications: What Are They? What of Them?" Acunetix.com. http:// www.acunetix.com/websitesecurity/web-applications/.

"What Is Cloud Computing?" Salesforce.com. http://www.salesforce.com /cloudcomputing/.

White, Gregory, Art Conklin, Chuck Cothren, Roger Davis, Dwayne Williams. *All in One Security+Certification Exam Guide*. Emery CA: McGraw Hill/Osborne, 2003.

Yager, Tom. "The Reality of Virtual Servers." Infoworld.com, 5 November 2004. http://www.infoworld.com/d/hardware/reality-virtual-servers-261.

AFRI AU PRESS
AIR FORCE RESEARCH INSTITUTE
http://aupress.au.af.mil