Information Society's Transformation into the

By: Nevin "Mustang" Taylor

I. EXECUTIVE SUMMARY

As we evolve from the Industrial Revolution into the information society, we are quickly learning how best to leverage knowledge as we step into the Age of Enlightenment. In this journey, we must ensure that we develop an information support mechanism that matures our Frame Of Reference (FOR) of how we see the world with an adequate perspective of our Situational Awareness (SA) to understand the dynamic, ever-changing environment in which current cloud endeavors are an attempt to address an increasing need for accessibility to information.

The necessity to provide this information in a timely and secure manner has been a topic of much discussion and great concern. As reliance upon this information increases, so does the growing threat from those endeavoring to access, deny or manipulate data. (Coram, 2002) With this in mind, this paper will explore the challenges of establishing a cloud infrastructure that provides non-repudiation for the data within our current infrastructure. Industry at all levels agrees that the most significant challenge in the cloud is providing a network capable of securing the integrity of data at rest, in transit, and throughout all phases of operations.

It is therefore crucial to establish confidentiality to build trust within the information environment. Only through sound policy and technological capabilities will the opportunity to attribute and hold accountable those accessing the cloud in our ongoing efforts to interlink and connect the world. Thus, this paper will address the evolving nature of this environment and outline the challenges associated with the inherent vulnerabilities and threats in this volatile, uncertain, complex, and ambiguous (VUCA) environment. However given the vast options and a plethora of opportunities the risk of doing nothing far outweigh the benefits to be derived from today's rapidly evolving information environment which is rapidly transforming us into the age of knowledge.

II. INTRODUCTION

The goal of information operations is as Sun Tzu advised, "The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but a few calculations beforehand." (Tzu, 2n Century BC) With this in mind we must look reflectively to clearly understand where we are to establish an enlightened pathway forward. To do this, the United States must evolve its current Information Technology endeavors with a focus on advancing cognitive processes. The current

environment is plagued by high latency. It is ill-equipped to sustain the current and future fidelity of knowledge essential to shaping our strategic perspective for success in our interlinked, information-dependent world.

Vivek Kundra, the U.S. Chief Information Officer, astutely understood the necessity to evolve the manner in which we store, access and leverage information. He established a Cloud First policy in the Federal Computing Strategy to address the growing need to leverage technology to unleash the power of information. (Kundra, 2011) The National Institute of Standards and Technology (NIST) in their Special Publication 800-145 defines "cloud computing as 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." (NIST, Cloud Computing (SP 800-145), 2011) the Federal CIO's new cloud strategy calls for the alignment of $20 billion of the $80 billion Information Technology (IT) budget to develop and implement cloud capabilities throughout the United States. (Kundra, 2011)

Given the ever-increasing demand placed upon the information environment and the necessity to integrate disparate systems in a way that precludes fragmentation, the Clinger–Cohen Act directs us to acquire technology in a manner that drives efficiencies and eliminates redundancies. (Franklin D. Raines, 1996) The implementation of cloud computing is a foregone conclusion, according to most experts, and, when done correctly, will provide greater accessibility and efficiency in information. With a rapidly increasing demand signal and ever-decreasing resources, cloud computing offers the opportunity to work smarter, not harder. Therefore, the focus of this paper will address how the cloud should be effectively and efficiently implemented to ensure the proper evolution and maturation of information that is both reliable and trusted. Thus, It is the trust one has in the quality of information and the trustworthiness of the systems that store and disseminate it that is at the heart of our ability to successfully make the necessary calculation to garner victory.

III. ASSETS OF VALUE

The Department of Defense Chief Information Officer acknowledges the challenges with implementing and integrating architectures that ensure the cloud provides the necessary security, continuity of operations and Information Assurance (IA) so essential to delivering reliable networks that provide for non-repudiation. *(Takai, 2012)* Joint Pub 6.0, Communications Systems, expresses the value technologies offer in the maturation of information. It provides the criteria for collecting, correlating, and fusing quality information, as outlined in Figure 1 below. Ultimately, for information to be of value, it must be accurate, relevant, timely, usable, complete, and secure. For these systems to be effective, they must be designed and integrated in a manner that leverages the criteria as established by the Federal Risk and Authorization Management Program *(Chief, 2010) (Fed RAMP).*

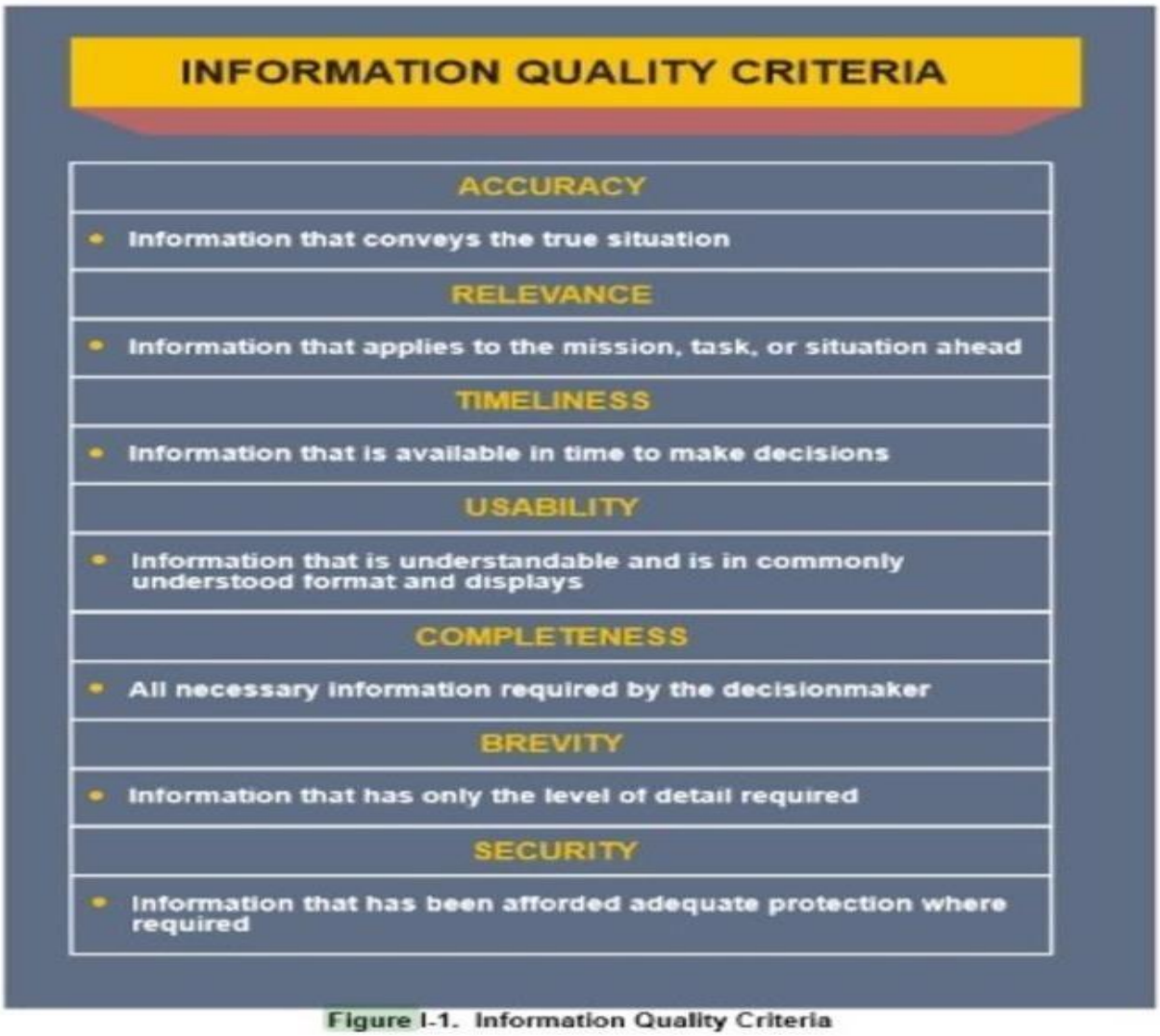


Figure I-1. Information Quality Criteria

The chart below (Figure 2) illustrates the relationships among controls, assets of value, design, and risk considerations within the security architecture that must be assessed to support mission requirements adequately. Policies must be put in place that establish the necessary controls to mitigate risk and ensure availability, integrity, and authenticity. Once accomplished, they will be able to determine the relevancy and assess the resulting confidentiality, non-repudiation, timeliness and veracity of the data. It is at this point that the value-added proposition of cloud becomes evident. With adequate measures to protect, detect, and correct attacks involving denial-of-service and malicious data manipulation, the capabilities inherent in the cloud to validate data and identify variance or inconsistency begin to reveal themselves. (Systems, 2006) (NIST, 800-59)

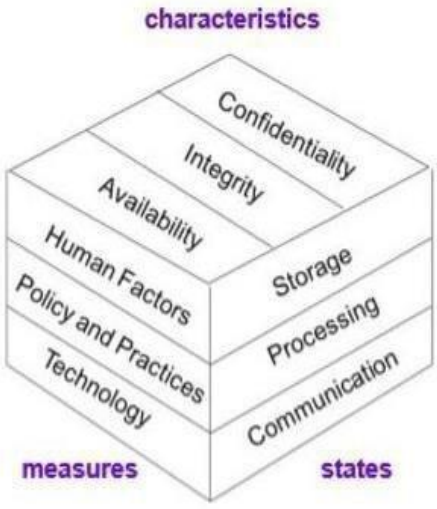
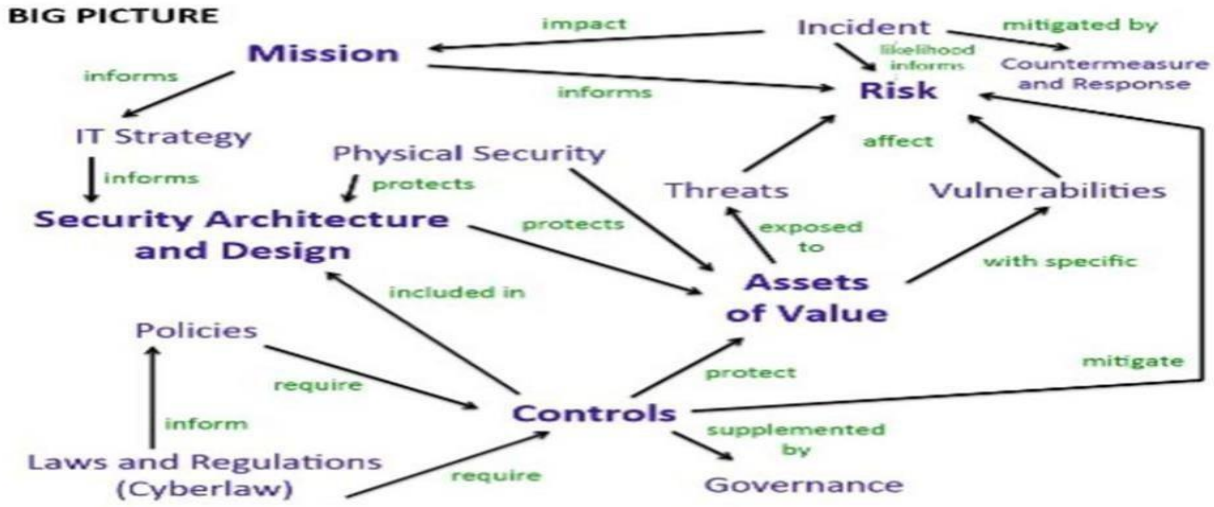


Figure #2: Characteristics, measures and state of data

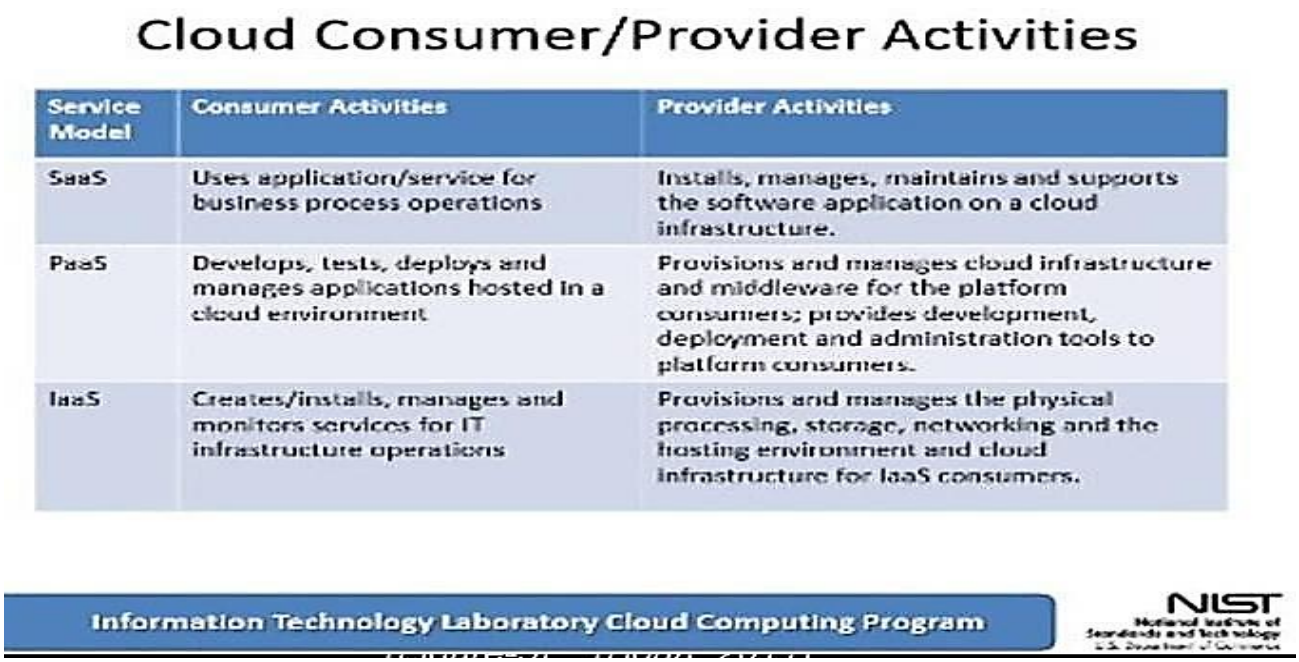
The greatest challenge of the cloud today is ensuring the confidentiality, integrity, and availability of data at rest and in transit, and across all aspects of operations. The McCumbers Cube provides an excellent pictorial representation of the building blocks of the information environment and the measures upon which the cloud must be built. The resulting dependencies and reliance upon people effectively leveraging technology with good tactics. techniques and procedures to ensure the collection, correlation, and application of reliable information in an understandable context. Through assessing the ebbs and flows of information while in storage, in transit, and during processing, the ways and means identify how best to mature data into information to ensure knowledgeable actions at the cognitive level of thought. (McCumber, 2004) Thus, protecting personal, diplomatic, privileged, military, and economically sensitive information is critical to establishing the system's credibility and, importantly, to gaining strategic advantage from the data it contains. Therefore, prudent steps should be taken to preclude unauthorized disclosure as outlined in CNSSI 4009. (CNSSI, Web Down)



(Figure-2 Duke, 2013)

V. VULNERABILITIES

Ultimately, the level of protection in both time and accessibility is directly related to the current and long-term value placed on the data. Therefore, mitigating risk by adequately detecting, protecting, and managing inherent cloud vulnerabilities must be a primary concern. It is through proper training of people, development of policy, and implementation of technology that ensures the necessary trust is established to provide the means to transform the information environment in a way that serves the US vital national interests. Ultimately, the responsibility to protect data resides with people who are unequivocally our greatest asset, and history has shown that through their actions or lack thereof, they have presented our most significant risk. Thus, a culture that is cognizant of actions taken to achieve results will be able to effectively leverage technology to preclude unauthorized access through well-established, clearly defined Tactics, Techniques, and Procedures (TTPs).



(Figure-5) (Bohn, 2011)

Bill Schaumann of the Global Technologies Study edifies that “Because you are in a virtual environment and data can be anywhere, a business user must be aware of all the different borders its data is crossing and the regulations that apply from each of those countries.” (Hyek). Furthermore, Paul Cabot highlights that “Underlying all the security and privacy issues is the concern that once it is shared, it will persist in that environment forever.” Therefore, the vulnerabilities of giving up control over data and the inherent regulations imposed by the jurisdiction where said data is stored have their own set of unpredictable limitations and unexpected consequences. (Hyek) For it is not merely adequate to establish policy that dictates where data may be stored while at rest, but must be given full consideration as to the implications of where said data traverses, the manner in which it is encapsulated before its transport, and the means by which it is processed. Only through well-defined TTPs can the information environment in order to prove an adequate baseline upon which to assess, detect, and protect against unauthorized access and malicious manipulation of data, and the prudent oversight of a well-defined Risk Management Framework (RMF) will be effective.

VI. THREATS

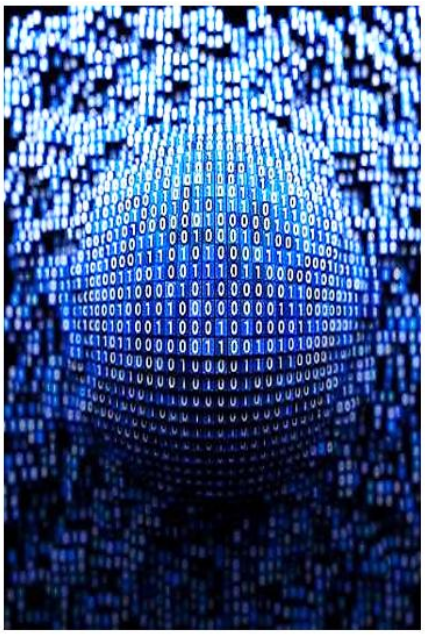
One of the greatest threats of this new medium, cloud computing, is the potential for network breaches and the information contained within. Early adopters of cloud computing have sought to develop TTPs and design their architectures to overcome these security concerns. (NIST, 7298, Website Down) Currently, past concerns about denial-of-service attacks and unauthorized access are being overshadowed by manipulation and loss of control over data at rest. The cloud's greater accessibility to information compounds the risk of the inherent veracity of data. This is merely one of many areas of concern, not the least of which is that data within the cloud environment has geographical boundaries. This raises questions about data ownership and control. Ernst & Young’s 2010 Global Information Security Survey identified that the “loss of control is rapidly emerging as the

number one inhibitor to adoption of public cloud computing services." (Hyek) These concerns, compounded by a recent survey by Global Technologies Industry, indicate that 36% of US and more that 57% of European organizations failed to adequately address risk concerns before migrating to the cloud. (Hyek) Ultimately, without positive control and accountability of data, and an effective RMF to sufficiently assess the impact of these threats, the resulting means to establish the necessary safeguards to protect and ensure mission assurance will continually leave at question whether it is prudent for an organization to migrate to the cloud.

Information is a commodity that is easily distributed, compromised, and manipulated. Today's increased reliance upon it makes it a vulnerable target to attack. Thus, it is essential that we measure it to determine what information it contains and to what level it must be protected, so that we can establish the level of confidence we can reasonably hold in it and thus the level of trust we have in it. Data at rest must be assessed to determine the impact of current risks despite available countermeasures to mitigate inherent vulnerabilities. Thus, the veracity of information impacts organizations in direct proportion to their reliance upon it. Therefore, once access is granted through trusted relationships, continual assessments must be conducted to determine at what level of confidence we can be assured that adequate measures are in place to defend against the growing threat of information warfare (IW).

Knowledge operators understand the clear and present dangers presented by ongoing IW and its insidious nature. Unlike cyber warfare, IW enables the adversary to gain access, acquire knowledge, and engage in disinformation campaigns without impunity. The anonymity of their action in most cases precludes attribution and thus allows them to disseminate and instantly devalue information's strategic value. Therefore, a trust but verify approach is necessary to ensure that actions taken are fulfilling and achieve the desired effects. Thus, authentication is essential to ensure that authorization provides attribution for actions, mitigating and attributing potential data manipulation or degradation of data at rest. (44, Web Page Down) (CNSSI, Web Down)

The ability to authenticate the identity of those on an access list becomes a crucial means to cross-correlate one's actions and authorizations against a dynamic trust criterion. To validate authenticity, biometrics enables positively correlating credentials with individuals. At the same time, cryptography provides a tool to secure data at rest for only those with a valid need-to-know. However, these tools lack the necessary capabilities; thus, new tools are needed to monitor data in transit, especially during application development, effectively. It is only through ongoing assessment of data across all three phases of its existence (rest, transit, and processing) that it identifies the actions necessary to protect and correct deficiencies, critical to adapting the system to mitigate risk and overcome threats as they arise. By providing a common site picture, the resulting baseline enables situational awareness and evolves our understanding of the information environment. It is through this standard matrix of correlating diverse perspectives on how to assess risk and the implications of the resulting causalities of actions taken to achieve results in this dynamic environment that we can better understand the impact we have within this fluid, ever-changing domain.



1. Organizations shall develop and maintain an ERM framework to manage risk to an acceptable level.
2. Formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. A similar assessment should be done for inherent and residual risk, considering all risk categories (e.g., audit results, threat and vulnerability analysis, regulatory compliance).
3. Risks shall be mitigated to an acceptable level and time frame, which shall be established and documented with executive approval.
4. Risk assessment results shall include updates to security and privacy policies, administrative procedures, standards and controls to ensure that they remain relevant and effective.
5. Once access risks have been identified and prioritized, a plan should be put in place to minimize, monitor and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls should also be implemented prior to provisioning access.

(Figure-6) (Hyek)

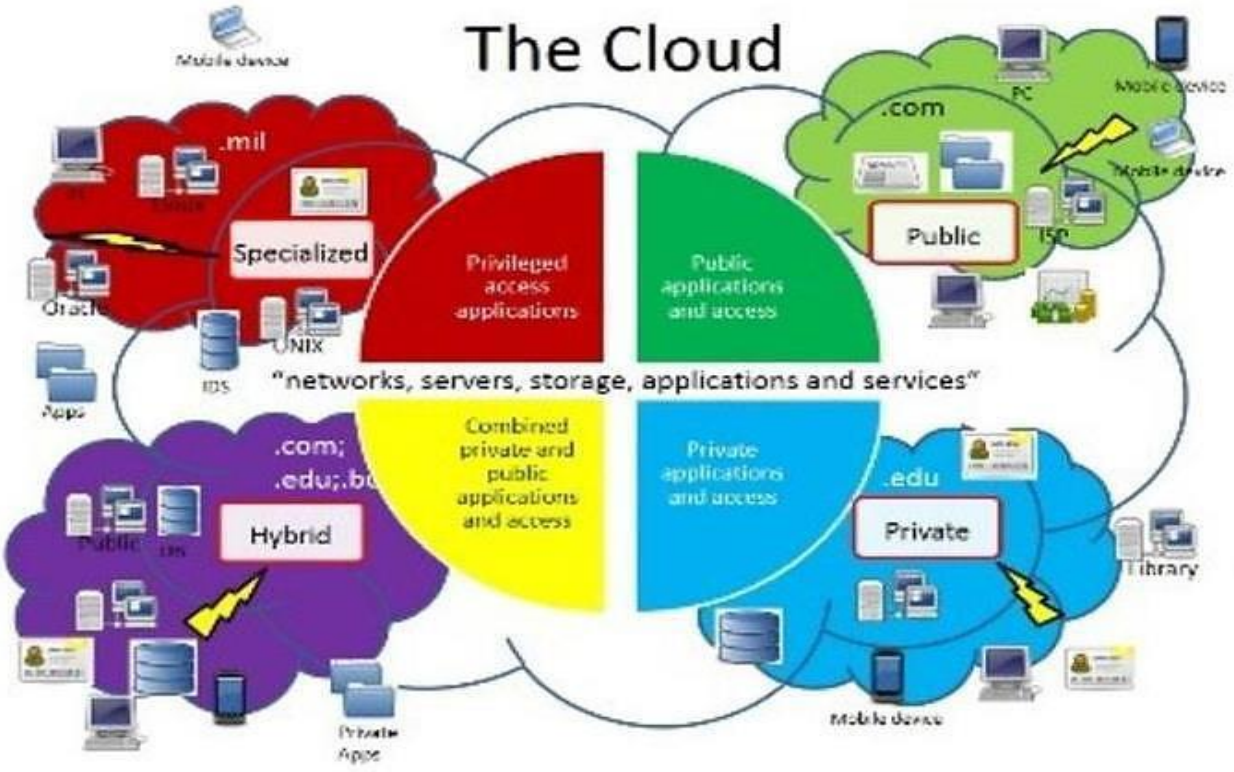
The conundrum of security concerns is a double-edged sword: the capabilities offered by the cloud can leave one potentially vulnerable. Even data contained on a private cloud, which is the least at risk given it is included and controlled within its own infrastructure, is still vulnerable. However, with appropriate policies and well-defined business rules and a well-designed architecture, it is feasible that highly confidential data like health, personnel or financial records can be safeguarded more securely through distributed storage. Overall, concerns about ownership and legal considerations for controlling data have garnered significant attention, and many efforts are underway to manage these threats and mitigate their impact. (Hyek)

OPPORTUNITIES

During a recent speech by the US CIO at the Brookings Institution in April 2010, he expressed concern that “Over the past decade, the number of federal data centers has grown from 432 to more than 1,100. This growth in redundant infrastructure investments is costly, inefficient, unsustainable, and has a significant impact on energy consumption,” (Hyek). Recently, the DoD initiated actions by publishing policies to address these issues. They are endeavoring to consolidate data centers to lower risk, increase efficiency, and provide a higher degree of reliability and resiliency, thereby improving capabilities in compliance with the Kling Cohen Act and the US CIO’s direction. (Clinger-Cohen, 1996) (Kundra, 2011)

Ultimately, these endeavors offer the opportunity to provide interoperability of equipment and applications for cross-domain services in accordance with the NIST standard. (NIST, Cloud Computing (SP 800-145), 2011) However, with this additional capability came an increased need for more robust security controls, through policy and architectural design, to protect classified information with varying security requirements across domains. (Takai, 2012) Through segmentation within the clouds as illustrated in Figure 7 below, the ability to establish private, specialized, and hybrid centers to ensure

confidentiality and security of information while providing a balanced approach toward accessibility proved to be highly effective in the application of their diverse set of mission requirements. However, it must be noted that the private cloud's isolation of data ultimately reduces accessibility, while the public cloud’s increased accessibility comes at the cost of increased vulnerabilities. Therefore, the hybrid version, while it affords the benefits of both worlds, also entails their unique risks.



(Figure-7) (Williams, 2010)

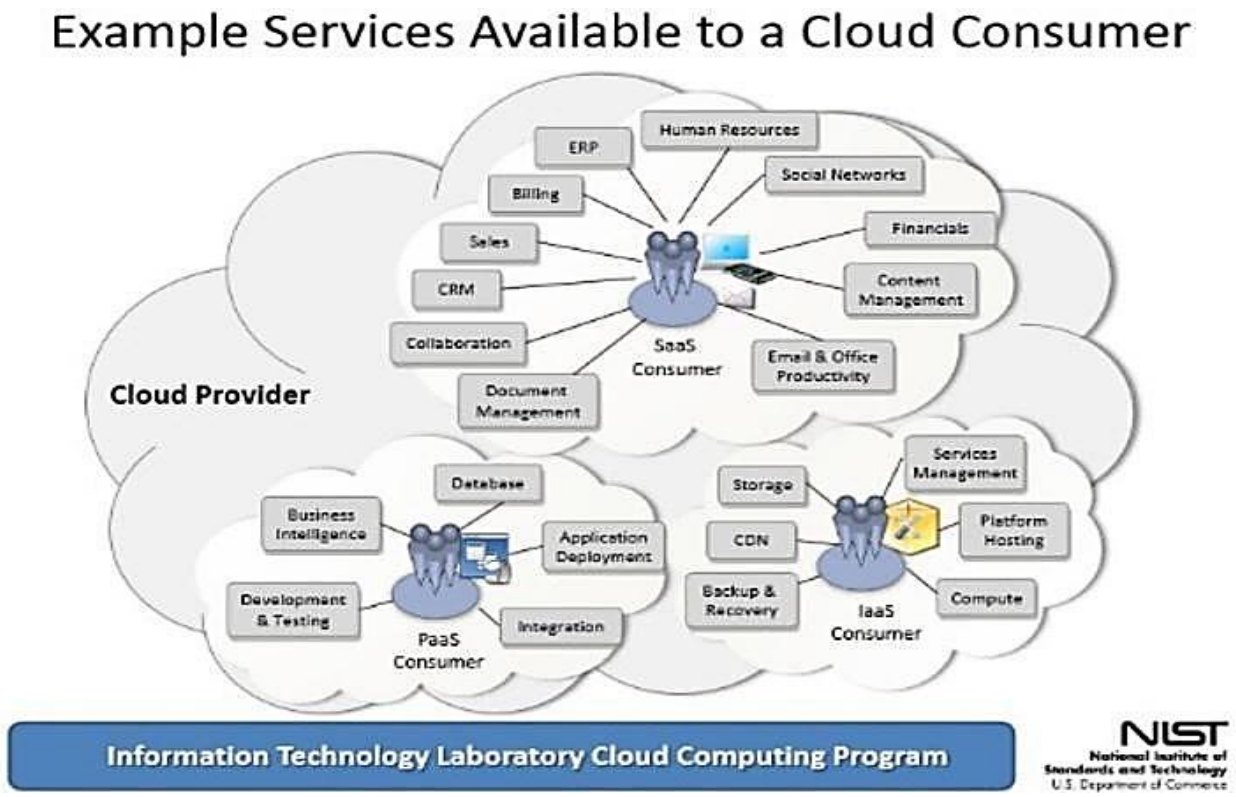
III. WAYFORWARD

As we endeavor to think about thinking in order to evolve understanding, we begin to realize that past actions affect current conditions, which in turn impact future results. Thus, by analyzing the commonalities and identifying differences in the data, opportunities to build on past actions and align them with future objectives emerge. Therefore, current efforts for data consolidation must be used as a catalyst to integrate all data to the cloud. Proper policies and well-defined architecture and training will ensure a responsible model is developed that provides the necessary flexibility to compartmentalize and distribute information in accordance with their need-to-know for both public and private communities of interest. For only in this manner will we be able to validate the knowns, learn about the unknowns and become aware of the unknowable. This approach is outlined in DoD’s Federal Cloud Computing Strategy, which identifies a plethora of benefits from efficiency of cloud services as illustrated by the table below. (Takai, 2012)

Efficiency	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data center Consolidation initiative) • Improved productivity in application development, application management, network, and end-user devices	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult to manage systems
Agility	
Cloud Benefits	**Current Environment**
• Purchase "as-a-Service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
Innovation	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-averse culture

The US CIO's enthusiastic support of the cloud foretells it to be the "intersection of higher processing power, cheaper cost and the ubiquitous access to broadband networks that for the first time can deliver content in ways that we couldn't imagine before ... transformation that's going to change the way we live our lives fundamentally." Despite the opportunities, many caution that caution should be exercised, given the tactical implications of early adoption of this new technology. (Petersen, 2010) Brookings Institution Cloud Computing is challenging traditional approaches to technology and offers the potential to drive collaboration and catalyze change in this area. The opportunity for agility to instantaneously adapt to requirements while providing on-demand accessibility and elastic storage capacity serves as a platform for a symbiotic partnership that increases capacity and efficiency by yielding a synergistic, asymmetric strategic advantage.

Fortunately, NIST's Cloud Computer Reference Architecture roadmap provides for a scalable, modular infrastructure to meet current and future needs. This document identifies security and privacy challenges and offers recommendations to support implementation planning at all levels of the organization. Tim Grance, the co-author reminds us that "Public cloud computing and the other deployment models are a viable choice for many applications and services. However, accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the organization to fulfill." (NIST, Special Pub 800-144, Web Down) Thus, the available services include Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), which are the three most common areas to consider when leveraging third-party applications such as email and office applications. (NIST, Cloud Computing (SP 800-145), 2011)

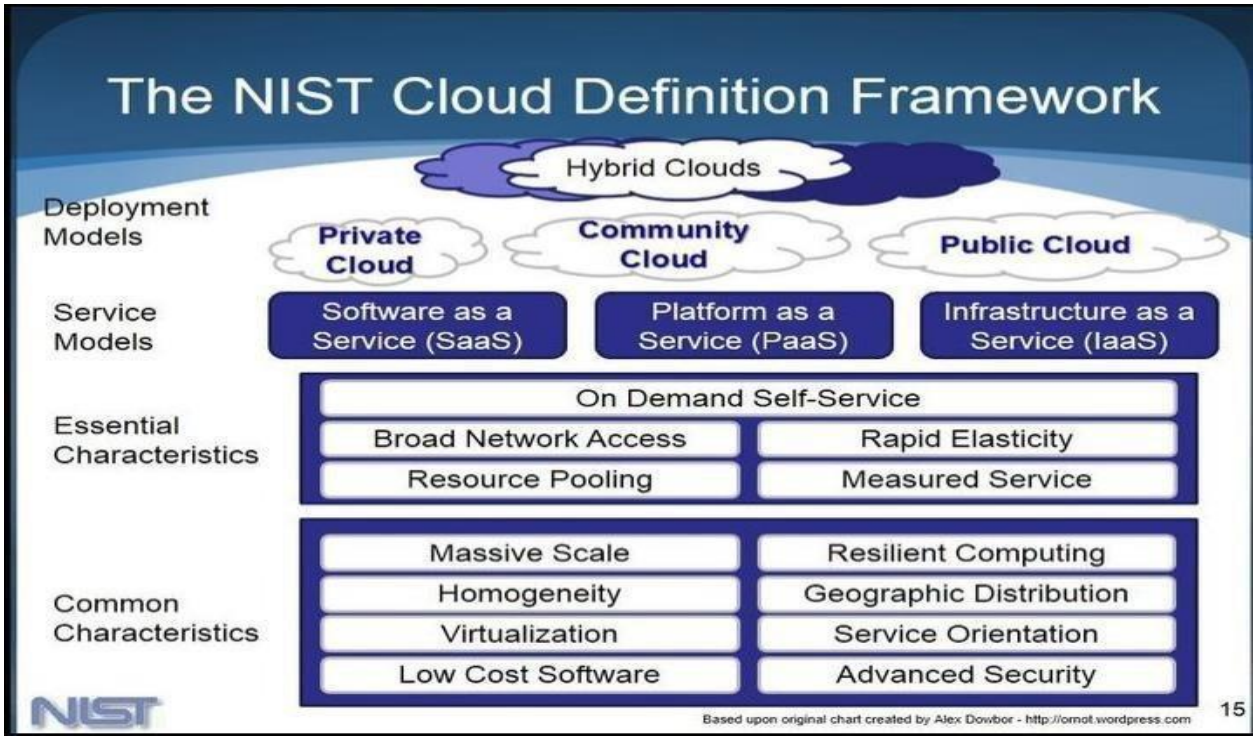


(Figure-9) (Bohn, 2011)

IX. IMPACTS

Cloud computing is increasingly accepted across the IT and business communities, beyond server virtualization and as a means for disaster recovery. The technology enables organizations to focus on the business at hand, undistracted by internal technological constraints. The new viewpoint of technology as a service affords them both the capability and capacity to purchase what they need when they need it. No longer will they have to manage technological infrastructure to provide the necessary capabilities to support elastic scalability and adaptability for current and future requirements. As the IT community evolve from a $12 billion industry in 2010 to a predicted $68 billion in 2014 it offers organizations the adaptive edge necessary to be competitive. The pending transformation of cloud computing will account for 15% of IT spending in 2010 and will continue to compound by 26% through 2014. (CIO, 2007) (Kundra, 2011)

The ability to link and drive collaboration is a synergistic catalyst for productivity. The singularity of focus to de-conflicted data precludes distraction within a wildly adaptive and often chaotic world stage. Thus, the functionality and diverse use of services to grow and expand is clearly illustrated by NIST's examples of services outlined in Figure 8 below and the SP 800-145 consumer activities report. (NIST, Cloud Computing (SP 800-145), 2011) The opportunity to have a viable backup and recovery mechanism to mitigate the impact of natural, technological, and malicious events on the organization can dramatically reduce downtime through application resilience. The results are consistently available in a pervasive Volatile, Uncertain, Complex and Ambiguous (VUCA) information environment.



(Figure 10 (Grance, 2009)

X. RECOMMENDATIONS

The importance of policy in establishing a cloud service that ensures adequate security and confidentiality depends on the network architecture. By integrating technology to ensure accessibility by authorized users, a baseline can be established from which to ascertain the level of trust that exists. To provide low latency and fulfill the demand for bandwidth in a safe and reliable manner, it is essential that a well-defined RMF and adequate TTPs be developed that are focused upon the fulfillment of mission objectives. By establishing clearly defined guidelines, the opportunity to develop and evolve the functionality that these technologies contribute helps to ensure prioritized access management, identity resolution, and standards for compliance and auditing requirements as outlined in Figure 11 below.

1. Federated security (e.g., identity) across clouds
2. Metadata and data exchanges among clouds
3. Standards for moving applications between cloud platforms
4. Standards for describing resource/performance capabilities and requirements
5. Standardized outputs for monitoring, auditing, billing, reports and notifications for cloud applications and services
6. Common representations (abstract, APIs, protocols) for interfacing cloud resources
7. Cloud-independent representation for policies and governance
8. Portable tools for developing, deploying and managing cloud applications and services
9. Orchestration and middleware tools for creating composite applications across clouds

(Figure-11)(Hyek)

By utilizing and complying with SAS 70 trust services to establish an assurance programs that use the tools within IOS 27001 and ISAE 3402 the requisite focus upon security that establishes trust within the network will allow building senior leaders' confidence through ongoing assessments, detection and maturation that limits the impact of malicious activity within the cloud. Additionally, standardized natural disaster recovery plans will ensure the resilience of large segments of data while alleviating concerns about the potential impact of intended and unintended consequences of cloud computing. NIST has prepared a draft 800-125 Guide to Security, which addresses these security concerns and provides a framework for establishing encryption to help alleviate the issues outlined in Figure 11 above. (Hyek)

A comprehensive architectural design and sound, well-thought-out plans, procedures, and policies will help prevent short- and long-term consequences from unforeseen events by distributing data and conducting continuous backups. This, coupled with consideration of the five characteristics and three measures as outlined in McCumber's cubic model, will ensure a comprehensive strategy to combat current and future threats. (Onwubiko, 2010) Endeavors to mitigate risk must be focused on operational implications, with the intent to preclude service degradation that minimizes capabilities, resulting in reduced confidence in data, loss of strategic advantage, or the long-term consequences of manipulated data. (NIST, FIPS 99, Website) Thus, cloud service providers must incur costs and be held liable and, in turn, accountable for mission impact resulting from inadequate maintenance or poor cyber hygiene.

There is no one-size-fits-all solution when it comes to cloud computing. Each architect, policy, and implementation must be custom-fit to the organization they support. Developing a means to address CIAAN concerns while providing the necessary resiliency to ensure current and future elasticity must be established and proactively evolved to serve as a catalyst that provides an asymmetric advantage on the field of battle. Reliability of backups, distributed operations, and adequate security measures will, over time, help build confidence and trust. It is through these efforts and the resulting efficiencies to be gained in this endeavor that must be capitalized upon to ensure the value- added proposition and operational sustainment is actualized. Overall, the opportunity to evolve and provide for the operational benefits far outweighs the risk incurred by transitioning to the cloud and thus bear serious consideration and our immediate attention. (Williams, 2010) (Amab Dutta, 2013)

References

07309295, C. R. (n.d.). Library and Information Sciences.

Chicago: American Library Association.44, T. (Web Page Down). U.S.C Section 3524. Amab Dutta, A. P. (2013). Risk in Enterprise Cloud Computing. Computer Information Systems, 39-48.

Bohn, R. (2011). NIST Cloud Computing Reference Architecture & Taxonomy Working Group. NIST. Washington DC: Department of Commerce. Retrieved from ***http://www.cloudstandardscustomercouncil.org/062011/presentations/NIST_RA_062111.pdf***

Chief, J. (2010). Joint Publication 6-0. Washing DC: Department of Defense.

CIO, A. (2007). Information Assurance (IA). Washington DC: Department of Defense. Retrieved February 21, 2013, from ***http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf***

Clinger-Cohen. (1996). Clinger-Cohen Act.

CLOUD COMPUTING AND BIG DATA INTERSECT AT NIST, JANUARY 15-17. (2012, Nov 30). US Fed News Service, Including US State News. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1220744129?accountid=12686***

CloudeAssurance, inc.; compiled for cloud consumers: Cloud security rating platform CloudeAssurance releases its 4th quarterly report entitled "top 10 CSPs". (2013). Infor Technology Newsweekly, 55. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1440306472?accountid=12686***

CNSSI. (Web Down). 4009. CODE, U. (n.d.). Title 44 Chapt 35. Code, U. (n.d.). Title 44 U.S.C Sec 3542. Coram, R. (2002). The Fighter Pilot who Changed the Art of War. New York: Back Bay Books.

Cracking open encryption standards (2013). . Washington, D.C.: National Public Radio. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1439417380?accountid=12686***

Das, P., Classen, H. W., & Davé, R. (2013). Cyber-security threats and privacy controls for cloud computing, emphasizing software as a service. Computer and Internet Lawyer, 30(3), 20-24. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1326330514?accountid=12686***

Duke, M. (2013, Oct). IAA Slides.

Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). RISKS IN ENTERPRISE CLOUD COMPUTING: THE PERSPECTIVE OF IT EXPERTS. The Journal of Computer Information Systems, 53(4), 39-48. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1429691370?accountid=12686***

FINAL VERSION OF NIST CLOUD COMPUTING DEFINITION PUBLISHED. (2011, Oct 26). US Fed News Service, Including US State News. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/900469193?accountid=12686***

Final version of NIST cloud computing definition published. (2011, Oct 25). Targeted News Service. Retrieved from***http://search.proquest.com.ezproxy6.ndu.edu/docview/900484042?accountid=12686***

Franklin D. Raines, D. (1996). Memoranda 97-02 (Funding Information Systems Investments). The White House, Budget, Office of Management. Washington: OMB. Retrieved from ***http://www.whitehouse.gov/omb/memoranda_m97-02/***

Ginovsky, J. (2013). A bank risk manager's view of the cloud. American Bankers Association.ABA Banking Journal, 105(6), 20-25. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1399965073?accountid=12686***

Grance, P. M. (2009). Effectively and Securely Using the Cloud Computing Paradigm. Washington, DC, USA. Retrieved from ***http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt***

Hyek, P. (n.d.). Cloud Computing Issues and Impact. Global Technologiy Industry Discussion Series, p. 56. Retrieved from ***http://www.ey.com/Publication/vwLUAssets/Cloud-computing_issues_and_impacts/$FILE/Cloud_computing_issues_and_impacts.pdf***

Information security; ron ross of NIST to keynote on cloud computing cyber security at vanguard security & compliance 2012. Defense & Aerospace Business, , 115. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1010539245?accountid=12686***

It's official: NIST defines cloud computing. (2011). Health Management Technology, 32(12), 6. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/912867449?accountid=12686***

Kundra, V. (2011, February 8). US Chief Information Officer. Federal Cloud Computing Strategy, pp. 1-37. Retrieved from ***https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf***

Leithauser, T. (2013). NIST ISSUES CLOUD SECURITY GUIDELINES. Cybersecurity Policy Report, , 1. Retrieved from ***http://search.proquest.com.ezproxy6.ndu.edu/docview/1412111122?accountid=12686***

McCumber, J. (2004). Assessing and Managing Security Risk in IT Systems. Boca Raton: Auerbach Publications.

Messmer, E. (2013). Panzura cloud storage controller gets NIST FIPS 140-2 certification for crypto. Network World (Online), Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/1312292260?accountid=12686

Montalbano, E. (2011). NIST releases federal cloud roadmap, architecture. Informationweek - Online, Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/889363386?accountid=12686

National institute of standards and technology NIST; 2 new publications provide a cloud computing standards roadmap and reference architecture. (2011). Computers, Networks & Communications, 61. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/893141552?accountid=12686

NIST. (2011, October 26). Cloud Computing (SP 800-145). US Fed News Service, Including US State News, p. all. Retrieved September 25, 2013, from http://csrc.nist.gov/publications/PubsSPs.html#800-145

NIST cloud computing videos available online. (2012, Feb 08). M2 Presswire. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/920210925?accountid=12686]

NIST cloud computing videos available online. (2012, Feb 07). Targeted News Service. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/920204522?accountid=12686

NIST issues cloud computing guidelines for managing security and privacy. (2012, Jan 25). M2 Presswire. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/917551863?accountid=12686

NIST issues cloud computing guidelines for managing security and privacy. (2012, Jan 24). Targeted News Service. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/917540616?accountid=12686

NIST october workshop to explore intersection of cloud computing and mobility. (2013, Sep 03). Targeted News Service. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/1429655156?accountid=12686

NIST. (Web sit down). FIPS 99. Washington DC: DISA.

NIST. (2011, October 26). Cloud Computing (SP 800-145). US Fed News Service, Including US State News, p. all. Retrieved September 25, 2013, from http://csrc.nist.gov/publications/PubsSPs.html#800-145

NIST. (n.d.). 7298 Rev.1.

NIST. (n.d.). 800-59. Washington DC: DoD. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf

NIST. (Web cite Down). 7298.

NIST. (Web Down). Special Pub 800-144. Washington DC: DISA. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-144/SP800- 144.pdf

NIST. (Web sit down). FIPS 99. Washington DC: DISA.

Onwubiko, C. (2010). Security Issues to Cloud Computing. Springer: London.

Petersen, S. (2010). The Impact of Cloud Computing Could Be Sky High - Eventually. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/1021792542/1413BA5F6FA7181C5E7/1?accountid=12686

Reilly, S. (2011). Cloud confidence needs new assurance standard. Computer Weekly, , 14. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/858387593?accountid=12686

Ross, P., & Blumenstein, M. (2013). Cloud computing: The nexus of strategy and technology. The Journal of Business Strategy, 34(4), 39-47. doi: http://dx.doi.org/10.1108/JBS-10-2012-0061

Sims, J. E. (2012). Information security in the age of cloud computing. (Order No. 3518361, The University of Mississippi). ProQuest Dissertations and Theses, , 171. Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/1033569848?accountid=12686

Systems, C. o. (2006). CNSS 4009. DISA. Washington DC: DISA.

Takai, T. (2012). Cloud Computing Strategy. CIO. Washington Dc: Department of Defense.

Taylor, N. (2009). SITUATIONAL AWARENESS—EVOLVING KNOWLEDGE INTO UNDERSTANDING: A COMPETENCY CRITICAL TO

US NATIONAL INTEREST. National Defense University, Joint Advanced War College. Washington DC: Defense Technical Institute. Retrieved from http://handle.dtic.mil/100.2/ADA530070

Trigueros-preciado, S., Pérez-gonzález, D., & Solana-gonzález, P. (2013). Cloud computing in industrial SMEs: Identification of the barriers to its adoption and effects of its application. Electronic Markets, 23(2), 105-114. doi: http://dx.doi.org/10.1007/s12525- 012-0120-4

Tzu, S. (2n Century BC). The Art of War. (T. F. Cleary, Trans.) Yinque Mountain: 1913. Ten best practices for the cloud. (2013). Network World (Online), Retrieved from http://search.proquest.com.ezproxy6.ndu.edu/docview/1367943181?accountid=12686

Walterbusch, M., Martens, B., & Teuteberg, F. (2013). Evaluating cloud computing services from a total cost of ownership perspective. Management Research Review, 36(6), 613-638. doi: http://dx.doi.org/10.1108/01409171311325769

Williams, M. (2010). A quick Start Guide to Cloud Computing. London.

Zlateva, P., Hirokawa, Y., & Velev, D. (2013). An integrated approach for risk assessment of natural disasters using cloud computing. International Journal Trade, Economics and Finance, 4(3), 134. doi: http://dx.doi.org/10.7763/IJTEF.2013.V4.273