NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT REPORT

SMARTER E-CONTRACTING: MOVING TOWARD BETTER SOURCING AND RETRIEVAL OF CONTRACT KNOWLEDGE

June 2021

By: **Jeremy Dedmon**
Georgette C. Hendricksen

Co-Advisor: **Brett M. Schwartz**
Co-Advisor: **E. Cory Yoder**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project Report

4. TITLE AND SUBTITLE
SMARTER E-CONTRACTING: MOVING TOWARD BETTER SOURCING AND RETRIEVAL OF CONTRACT KNOWLEDGE

5. FUNDING NUMBERS

6. AUTHOR(S) Jeremy Dedmon and Georgette C. Hendricksen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This project reviews the current contracting storage method for contracts and supporting documentation of contracts in the United States Air Force (USAF) and Department of Defense Education Activity (DODEA). The project explores the history of cloud computing within the government as well as the commercial marketplace. An in-depth analysis of current contracting systems within USAF and DODEA is completed, which shows that our current generation of contracting systems hinders the standard contracting professional's ability to retrieve data from other government entities. The paper further explores what is currently state of the art within the commercial realm in document generation and storage. This approach gives an accurate picture of where the government is currently lacking in its ability to share information internally. This paper results in four separate recommendations for the reader to consider. The recommendation that is most effective in terms of technical capabilities and cost constraints is for the government to continue down its current path of system development. While continuing this development, the government should consider expanded accessibility and compatibility of these systems.

14. SUBJECT TERMS
contracting, e-contracting, cloud computing, Department of Defense Education Activity, DODEA, United States Air Force, U.S. Air Force, USAF

15. NUMBER OF PAGES
79

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SMARTER E-CONTRACTING: MOVING TOWARD BETTER SOURCING AND RETRIEVAL OF CONTRACT KNOWLEDGE

Jeremy Dedmon, Civilian, Department of the Air Force
Georgette C. Hendricksen, Civilian, DOD Education Activity

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CONTRACT MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Brett M. Schwartz
Co-Advisor

E. Cory Yoder
Co-Advisor

Rene G. Rendon
Academic Associate, Graduate School of Defense Management

THIS PAGE INTENTIONALLY LEFT BLANK

SMARTER E-CONTRACTING: MOVING TOWARD BETTER SOURCING AND RETRIEVAL OF CONTRACT KNOWLEDGE

ABSTRACT

This project reviews the current contracting storage method for contracts and supporting documentation of contracts in the United States Air Force (USAF) and Department of Defense Education Activity (DODEA). The project explores the history of cloud computing within the government as well as the commercial marketplace. An in-depth analysis of current contracting systems within USAF and DODEA is completed, which shows that our current generation of contracting systems hinders the standard contracting professional's ability to retrieve data from other government entities. The paper further explores what is currently state of the art within the commercial realm in document generation and storage. This approach gives an accurate picture of where the government is currently lacking in its ability to share information internally. This paper results in four separate recommendations for the reader to consider. The recommendation that is most effective in terms of technical capabilities and cost constraints is for the government to continue down its current path of system development. While continuing this development, the government should consider expanded accessibility and compatibility of these systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARPANET	The Advanced Research Project Administration
AWS	Amazon Web Services
CAR	Contract Action Report
CLS	Clause Logic System
CON-IT	Contracting Information Technology System
CONWRITE	Contract Writing System
CSA	Client Service Administrator
DEAMS	Defense Enterprise Accounting and Management System
DISA	Defense Information System Agency
DOD	Department of Defense
DoDEA	Department of Defense Educational Activity
DPC	Defense Pricing and Contracting
EC2	Elastic Compute Cloud
EDA	Electronic Documents Access
ERM	Electronic Records Management
FCCS	Federal Cloud Computing Strategy
FedRAMP	Federal Risk and Authorization Management Program
FPDS-NG	Federal Procurement Data System-Next Generation
FY	fiscal year
GAO	Government Accountability Office
GPF	Google Cloud Platform
HPCC	High-Performance Computing Cluster
HVA	High Value Asset
IaaS	Infrastructure as a Service
iSCSI	Internet Small Computer System Interface
IRAPT	Invoicing, Receipt, Acceptance, and Property Transfer
IT	Information Technology
LAN	Local Area Network
NASA	National Aeronautics and Space Administration
NFS	Network File Server

NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PaaS	Platform as a Service
PD2	Procurement Desktop-Defense
PWS	Performance Work Statement
RACE	Rapid Access Computing Environment
SaaS	Software as a Service
SAN	Storage Area Network
SEC	Securities and Exchange Commission
SF	Standard Form
SLA	Service Level Agreement
USAF	United States Air Force
VAO	Virtual Acquisition Office
VPN	Virtual Private Network
WAWF	Wide Area Workflow

I. INTRODUCTION

A. SCOPE

This thesis explores the conceptual implementation of a better sourcing and retrieval contract repository for two Department of Defense (DOD) organizations: the Air Force and the DOD Education Activity (DoDEA). This thesis recounts the history of what has been in use and what is currently in use, and discusses positive and negative dimensions of the various approaches concluding with a recommended and most beneficial model for implementation.

B. PRIMARY AND SECONDARY QUESTIONS

1. Primary—Smarter E-Contracting—Can Contracting Knowledge Be Better Sourced to Allow for Instantaneous or Near-Instantaneous Sharing of Data?

With the ever-changing nature of technology, many products and concepts are outdated before they even hit the consumer marketplace. This makes it imperative for any enterprise to be fluid with their technological infrastructure. One of the growing trends and emerging technologies in the IT industry is the idea of cloud computing. It seems that all that is heard today from all different sectors of industry is the desire or plan to move services to the cloud.

With the cloud, data is readily accessible making information instantaneous to access from anywhere an internet connection is available. This quick access of information may lead to increased sharing of unique experiences and better prepare any career field for future challenges. This solution needs to be further explored by the government to ensure that all aspects of the government are operating on the highest level they can.

2. Secondary Question 1—Why Is This an Important Topic and What Is the Background of Cloud Computing?

The reader needs to understand what is meant by cloud computing. This treatise aims to define exactly what is the definition of cloud computing. This will be done by

exploring different characteristics, service and deployments models, and the advantages and disadvantages of cloud computing. While defining exactly what cloud computing is, there should be a clear indication on whether it can be and should be utilized in todays and future government contracting.

Additionally, current and past government policies need to be explored. This data gives the groundwork of how the government has arrived in its current situation. Policies provide government officials the groundwork to procure advanced technologies and services. The policies for cloud computing should provide similar guidance for cloud computing. The policies set forth by the government should detail the advantages, disadvantages, and risks of the service. It should also detail or provide suggestions on how to mitigate the risks. Lastly, policies should provide assistance in determining what programs or locations are the best candidates for the new service or technology.

3. Secondary Question 2—What Is Currently Being Utilized in the Government and Commercial Marketplace? Where Do the Current Systems Lack in Capability and What Could be Implemented?

In order to define whether it should be used, the current contracting systems in the government need to be analyzed. This thesis will specifically assess systems that are currently being utilized by USAF and DoDEA. The analysis will cover the strengths and weaknesses of each system along with the type of IT system each system entails. This analysis should show whether a current system being utilized within the government can be modified or transitioned to cloud computing software.

This thesis explores the current cloud computing offerings in the commercial marketplace. This exploration helps give the readers a rudimentary foundation of cloud computing capabilities in the commercial marketplace. Our findings will assist in answering our primary question to determine if the government is in an advantageous position to utilize their own individualized systems or those available in the commercial marketplace for their cloud computing needs.

Lastly, the security of cloud computing needs to be heavily scrutinized in any recommendation to utilize cloud computing. With the current state of affairs in the world,

more and more warfare is orchestrated not on the battlefield, but in cyberspace. Since cloud computing is entirely network based, the security of the system is paramount when considering alternatives. The last thing that anyone would want to do is open the U.S. federal government to a large-scale cyber-attack due to security that is lacking or easily breached. Accordingly, our secondary question is, given what the research tells us, can the U.S. federal government obtain a sourcing and retrieval contract repository that can provide the rigorous security requirements necessary to sustain such a system.

C. THESIS OVERVIEW

This thesis introduces the definition of cloud computing, its characteristics, the type of service models currently in effect, and the deployment models in operation in the workplace environment. The thesis also cites the federal government's stance on cloud computing and discusses the advantages and disadvantages of utilizing this model for data storage.

Additionally, the thesis discusses the current government contract documentation storage systems in place as well as contrast them with the current commercial storage and data systems. In addition, this thesis includes a discussion of emerging technologies and trends in the cloud computing world.

This thesis serves to provide the strengths and weaknesses of the current government procurement data storage systems as well as conduct further analysis based on the researchers' findings for the feasibility of government cloud computing for data storage. The thesis closes on what improvements the government can make in this area for more efficient contract documentation preservation and security.

Lastly, this thesis takes all the information found and provides three recommendations for consideration in the near future. Each recommendation is supported by findings that were explored previously in the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. INTRODUCTION

This chapter introduces the definition of cloud computing, its characteristics, the type of service models currently in effect, and the deployment models in operation in the workplace environment. The chapter also cites the federal government's stance on cloud computing and discusses the advantages and disadvantages of utilizing this model for data storage.

B. WHAT IS CLOUD COMPUTING?

The National Institute of Standards and Technology (NIST) 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" (Mell & Grance, 2011, p. 2).

According to Mell & Grance (2011) there are five characteristics of a cloud model. These characteristics are

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service (p. 2).

1. Service Models

Mell & Grance (2011) further indicate these three service models for a cloud model.

- Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
- Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (pp. 2-3)

2. Deployment Models

Mell & Grance (2011) explain that there are also four deployment models for the cloud model.

- Private cloud. The cloud infrastructure is provisioned for 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.
- 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.
- 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.
- Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). (p. 3)

According to the Federal Cloud Computing Strategy (FCCS), the purpose of cloud computing is to allow IT systems to be scalable and elastic. This is due to the ability to scale up and down cloud computing resources instead of needing to purchase all the resources necessary to run a new program or increase number of users. An example of this efficiency is the NASA Nebula program. This program gives researchers the ability to access IT services in minutes as opposed to the old method of procuring and configuring the IT resources. (Kundra, 2011).

C. ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING

There are many documented advantages of utilizing cloud computing. These advantages range from cost to reliability.

1. Cost

In the Congressional Research Report by Figliola and Fischer (2015), the considerations for cost when adapting to cloud computing are detailed. Due to the efficient utilization of resources, many times a significant cost benefit is realized when utilizing cloud computing as opposed to maintaining servers in a central or on-site location. The report explains that cloud computing works by allowing an end-user to purchase only the computing power used; therefore, an end-user is not required to purchase all the hardware to run a program that may only be utilized a fraction of the time. Another advantage that cannot be overlooked is the reduction of financial burden when implementing a brand-new application. Figliola and Fischer indicate that by maintaining a server farm, end-users are required to purchase the required processing power to run any new application and programs they would like to run. Doing this can be a risky venture because if the application is a failure all the additional investment in infrastructure becomes dead costs. With cloud computing, an end-user merely pays for additional computing power for the new application. If the application is a failure, then the end-user simply reduces the computing power utilized on the cloud. This makes implementing new applications and programs less risky thus allowing the end-user to be more aggressive in the IT arena.

Figliola and Fischer (2015) contend that while most believe that the cloud will result in a cost savings, one item that is consistently looked upon as a potential significant cost driver to the end-user is the migration of data and the time that is associated with transitioning or moving the data. Depending on the size of the organization and the number of users and types of data, migration may take up to a year. In addition, if soliciting for a provider, government procurement requirements need to identify and factor in a data migration plan as a part of the submittal requirement. The report adds simple data migration consists of a data format that is not very expensive to migrate. However, documents that will need to be converted to a new format will be very costly to the end-user. In addition, the size and number of files would also increase the cost the end-user should expect to pay. The authors further note another risk to cost occurs when the company that is being contracted to provide the cloud services is going out of business. If

this were to happen the end-user would need to find a new company to contract with as well as pay to have the existing data migrated to a new cloud and a new hosting company.

2. Energy Savings

Figliola and Fischer (2015) also address energy savings when adapting the cloud computing. Whether moving to the cloud or not, energy efficiency is a highly debated topic. The Figliola and Fischer report indicates that the size of the organization going to the cloud seems to matter; the smaller the organization, the more energy efficient moving to the cloud becomes. This advantage is because the amount of power utilized in a local server farm that is only utilizing a small portion of the storage is much larger than what power is utilized on that small section of the cloud. Another argument is that the manner in which many cloud providers ensure reliability reduces any of the energy advantages the cloud may or may not have been able to provide. Lastly, items that require special computing needs and hardware also tend to be less energy efficient and cost more to switch to the cloud.

3. Availability

The report by Figliola and Fischer indicates cloud computing allows programs to become more available to all users due to the program only being installed in the cloud allowing each user to connect to the program via the internet. This is opposed to the historically used method of installing each program on each individual system. Currently, if an application, such as PD2, is not installed on your system you will not be able to access the program and complete any contracting action.

While this is a strength, Figliola and Fischer (2015) argue that the cloud's dependence on an internet connection is also a weakness. Anybody who has worked for the government can attest government internet systems are notorious for being unreliable compared to its commercial counterparts. If a unit is relying on the cloud to run all of its programs, anytime an internet connection cannot be established, no work can be completed in any of the programs. In the contracting career field, this is less of an issue because the current programs, while not on the cloud, still require an internet connection to run. This is due to their connections to external systems.

Furthermore, the authors argue that the availability of the cloud could affect teleworking agencies. As the cloud requires a consistent broadband connection, the report concludes many people who live in rural America may not be able to access the cloud. Further research would need to be implemented at organizations that allow or encourage telework to ensure all employees teleworking have sufficient internet connections.

4. Agility

The Congressional Research Report by Figliola and Fischer (2015) notes that for many standard computing applications, the cloud can provide a more agile solution to computing needs. The cloud can provide this by providing more efficient use of upgrades and technological advances. By having the program on the cloud, any updates to the program only need to be done on the cloud and not each individual system that runs the program.

Figliola and Fischer (2015) insinuate that the cloud presents an issue with portability and interoperability of data. Cloud providers may not be easily switched due to issues with the interoperability of data on each cloud infrastructure. The report asserts if data is not interoperable with a new cloud infrastructure, the government will need to modify the data to become interoperable. This then increases a potentially expensive porting process to transfer data. This becomes a concern if the government is not creating its own cloud infrastructure but utilizing a commercial source. Commercial sources can go out of business at any time or their contract can expire. In these cases, the government would then have to port the data to a new system which would result in additional and unexpected costs associated with the cloud.

5. Security

Figliola and Fischer (2015) support that the cloud has similar vulnerabilities to that of a system of local computers. The data in the cloud is vulnerable to both internal and external threats and vulnerabilities in operating systems and programs need to be addressed as to whether the cloud or local computing is utilized. The report further indicates cloud storage differs when the concept of economies of scale come into play when data and programs are stored on the cloud. Since all the important data is located on the cloud the

resources utilized to secure each system can now be reallocated to the cloud. This would allow the user to more effectively utilize security resources. However, with all the contract data in one or a small number of locations this makes the cloud a larger target than each individual local computing station. The authors argue that this concentration of data allows those who are looking to steal the data in a cyberattack the ability to consolidate their resources as well to attack and access one central location.

The report also concludes that the cloud creates confusion on who is responsible for security. If a public company is leveraged to provide cloud storage, there is ambiguity on who is the responsible party for ensuring the security of the data. This is especially true with the government which has more stringent security requirements than many public entities. If a contract was written for cloud storage, then the contract would have to contain clear verbiage on who is responsible for security and what level of security is required on the cloud. This also presents a concern on the number of vendors that could potentially provide cloud services to the government.

Lastly, Figliola and Fischer (2015) suggest that the degree of legal protection for information in the cloud is up for debate, especially if a public cloud is utilized. The legal concerns go up depending on the country that the servers are stored. The reports explains that each country may have different data laws that may protect companies for not providing sufficient security. This is also true within the United States as each state has their own laws that may alter the protection afforded to the data.

6. Reliability

Additionally, the report by Figliola and Fischer (2015) discusses the potential impacts that cloud computing may have on reliability of service. The report points out that when data is spread among multiple data centers and is combined with redundancies, it tends to become more reliable. The research completed by Figliola and Fischer seems to agree that cloud computing downtimes have been rare, and many consider cloud computing to be more reliable than local computing.

Reliability needs to be included in the contract with clearly definable terms of reliability. These could include uptime, number of servers, or guaranteed response and

resolution times (Figliola & Fischer, 2015). This allows the user to hold the service provider accountable for any downtime that is excessive in nature.

7. Privacy

The final consideration of cloud computing discussed by Figliola and Fischer is privacy (Figliola & Fischer, 2015). As of writing their report laws had yet to be updated to specifically protect data in the cloud. This particularly comes into play for data that is stored on public and hybrid clouds. The report states that the government law for this type of data is the Electronic Communications Privacy Act of 1986. It is further indicated that this law is difficult to understand and leaves gaps for common services such as email and documents created and stored in the cloud. This is attributed to the fact that the cloud had not even been considered a possibility at the time the law was enacted. Until laws are created to specifically protect data in the cloud, privacy concerns will continue to be a hot issue.

D. A BRIEF HISTORY OF CLOUD COMPUTING

To many outside of the technology career field the cloud seems to be a recent phenomenon; within the IT realm, every company seemingly is touting what they can do in the cloud. The truth is that the term "cloud computing" has showed up as early as 1996 when it was utilized in an internal document at Compaq, a now-defunct tech company (Williams, 2018). While that is the first known usage of the term cloud computing, the idea of shared resources for computing had been around for decades.

The first known example of working model that follows the definition of cloud computing was The Advanced Research Project Administration or ARPANET in 1969 (Williams, 2018). This system was established by the United States government and interconnected four university computers as a way to share resources for scientific purposes (Williams, 2018). This system eventually evolved into an early predecessor of the internet (Williams, 2018).

Technological advances in cloud computing technology remained fairly stagnant or unknown through the 1970s. However, in the 1980s we started seeing supercomputing

centers start to form (Williams, 2018). The National Science Foundation began the initiative to build these sites as a national backbone network based on transmission control/ internet protocol (Williams, 2018). In the mid-1980s network access to these supercomputer sites were created leading to the start of commercial Internet Service Providers in the late 1980s (Williams, 2018).

In 1990, Tim Berners-Lee invented the World Wide Web making the online internet visible to all (Williams, 2018). While the internet continued to develop through the 1990s, the next major development for cloud computing occurred in 1999. Salesforce.com launched its services becoming the "pioneer in delivering enterprise applications via the cloud, now known as Software-as-a-Service." (Williams, 2018). The applications were accessible via the internet and ran in the cloud allowing large number of customers while lowering costs (Williams, 2018). Around this time, other services from more mainstream companies became available. In 2002, Amazon launched Amazon Web Services (AWS) and in 2006 launched Elastic Compute Cloud (EC2) (Williams, 2018). AWS delivered a suite of cloud-based services that allowed customers to only pay what they utilized (Williams, 2018). EC2 allowed for users to compute in the cloud for the first time commercially which increased the computing resources at a user's hands (Williams, 2018). In 2008 Google launched the Google App Engine which was a Platform-as-a-Service cloud and allowed "developers to host web application in its managed data centres." (Williams, 2018).

Gartner, the analyst house claimed that cloud computing "would become 'as influential as e-business'" (Williams, 2018). They also claimed that the concept would take many years to mature but would not just be the next generation of the internet (Williams, 2018). Additionally, Gartner pointed out that the term had or was being used under multiple definitions which caused some confusion (Williams, 2018). "Gartner described cloud computing as 'a style of computing in which massively scalable IT-related capabilities are provided as a service using internet technologies to multiple external customers." (Williams, 2018).

In 2010, Microsoft launched Azure, which helps streamline the development of web and mobile apps and is currently used for building, testing, deploying, and managing

apps through Microsoft data centers (Williams, 2018). Also, in 2010 Rackspace OpenStack released as a free open source platform for cloud computing (Williams, 2018). IBM launched SmartCloud in 2011 which provides technologies allowing for users to build different types of clouds (Williams, 2018). Google's Compute Engine, which allows users to launch on demand virtual machines from standard or custom images, launched in 2013 (Williams, 2018). This marked the last major launch of cloud computing technologies.

Gartner's analysis leads to the thought that cloud vendors will look at technologies machine learning to gain the upper hand on competitors (Williams, 2018). Additionally, it is predicted that $411 billion will be made in revenue for cloud services in 2020 (Williams, 2018). Lastly, Gartner's research director Sid Nag states, "In the IaaS segment, Amazon, Microsoft, and Alibaba have already taken strong positions in the market. In the SaaS and PaaS segments, we are seeing cloud's impact driving major software vendors such as Oracle, SAP, and Microsoft from on-premises, license-based software to cloud subscription models" (Williams, 2018).

E. CURRENT GOVERNMENT POLICY

On 8 February 2011, The White House released the FCCS, written by Vivek Kundra, which instituted guidance for the federal governments Cloud First policy (Kundra, 2011). The intent of this policy is to force government agencies to evaluate cloud computing as an alternative when procuring IT and in the budget process. The FCCS provides guidance to the definition of cloud computing which mimics the definition that is provided by NIST, benefits of cloud computing, recommended processes for making the decision to migrate to the cloud, case studies for cloud migration, and discusses risks associated with migrating to the cloud.

Figure 1 shows the benefits of the cloud compared to the current environment in three key areas, efficiency, agility, and innovation (Kundra, 2011). The FCCS indicates that these are the areas the government is most likely to benefit from by migrating to cloud computing. These areas benefits will be recognized "through more effective use of IT investments, and by applying innovations developed in the private sector."

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	• 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-adverse culture

Figure 1. FCCS Cloud Benefits. Source: Kundra (2011).

The FCCS provides federal agencies with a framework to make the decision to move programs to the cloud (Kundra, 2011). The three recommended phases of the framework are to select services to be migrated, provision the cloud services, and manage as a service not asset. Figure 2 shows a simplified version of the framework. Figure 3 shows how to select services for cloud migration based on the readiness (security, government readiness, life cycle of the program, etc.) of the program and value (efficiency, agility, and innovation) to move to the cloud.

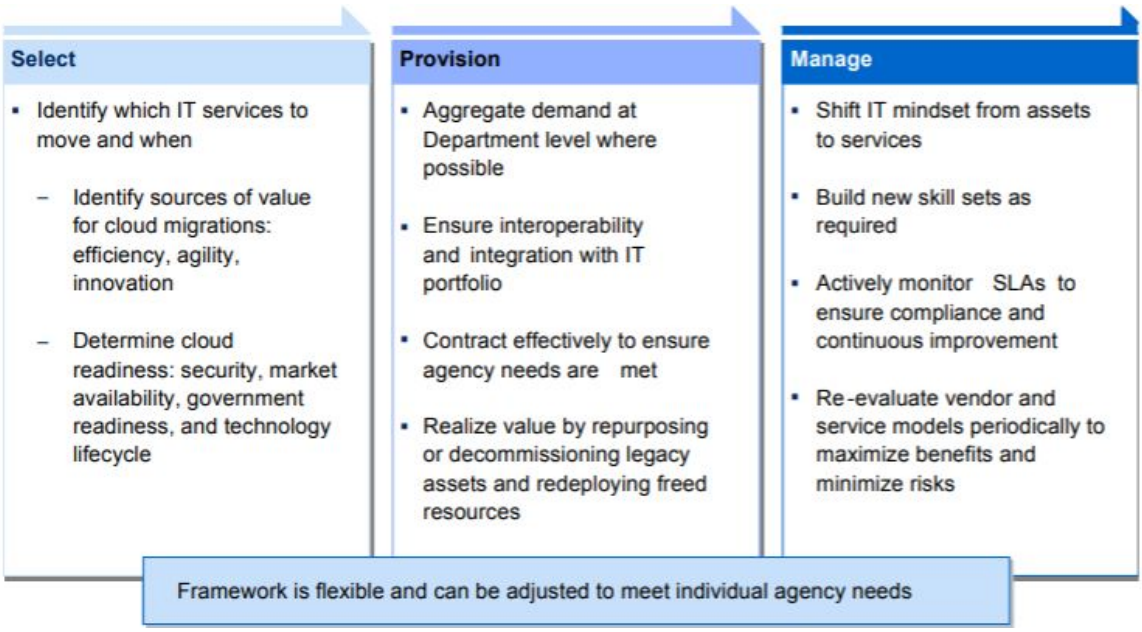

Figure 2. Three Stage Framework for Cloud Migration.
Source: Kundra (2011).

In relation to this thesis, Figure 2 and Figure 3 would help a program office determine if the contracting systems were ready to shift to cloud computing and whether contracting systems should be a first mover to the cloud. Contracting systems have already started to move to the cloud with the newer contract writing systems that have been released. In the realm of the government as a whole the contracting systems were ready to move as a vast majority of the contracting process exists on computers and over the internet. Additionally, based on these figures contracting systems would have been considered a medium-term mover. This is determined by at the time of the release of this policy the contracting systems were not ready to move to the cloud but there was high value in moving the systems to the cloud. The value in moving contracting systems to the cloud is the ability to connect to the contracting system from anywhere increasing the ability for workers to work from anywhere.

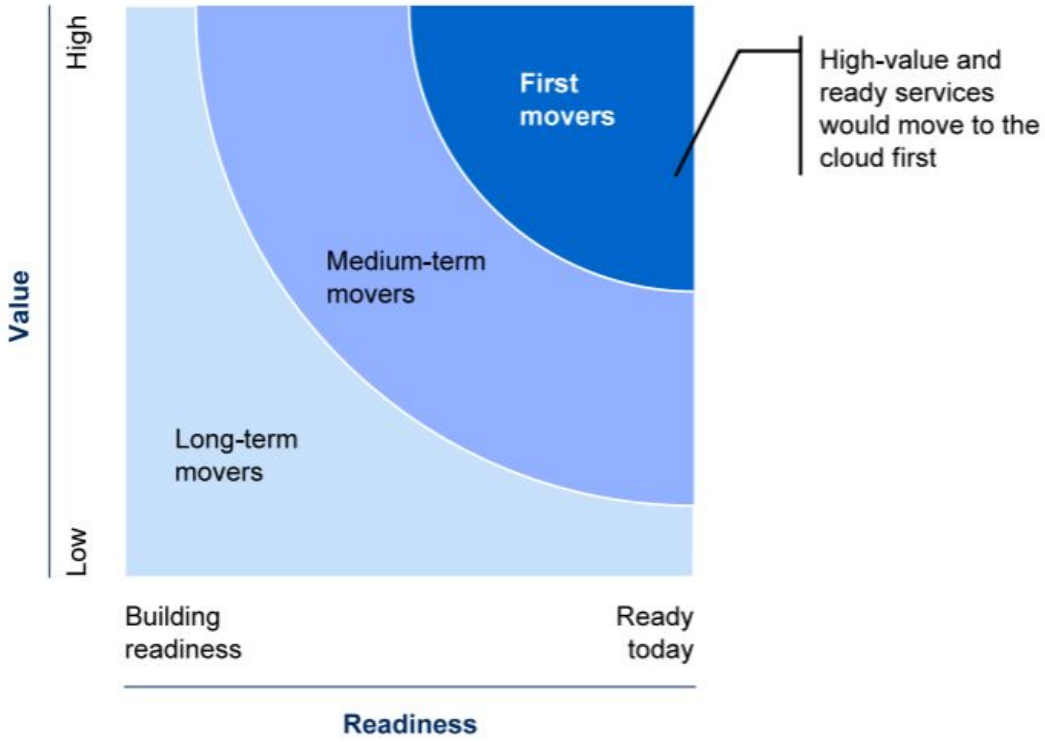

Figure 3. Services to Migrate to Cloud. Source: Kundra (2011).

Per the FCCS, organizations need to identify the value and readiness of a program to ensure it is a good candidate for cloud migration (Kundra, 2011). Value refers to the efficiency, agility and innovation that cloud computing provides the program. Efficiencies tend to have an impact on the bottom-line cost of a program by utilizing computer resources more efficiently, reducing IT support costs, and reducing capital investment costs. Agility comes in the form of being able to rapidly deploy new or upgraded computing resources opposed to purchasing new assets. Innovation refers to the need for the program to continue to improve in the future, or in the case of established commercial practices, if the cloud is being used for these services by the commercial marketplace. By combining these three factors an organization should be able to provide an estimation on the value for cloud migration of their program.

The FCCS indicates readiness refers to the programs ability to quickly migrate to the cloud based on both program and cloud related factors (Kundra, 2011). The factors can

include, but are not limited to, service characteristics, market characteristics, network infrastructure, application and readiness, government readiness, and technology life cycle.

The FCCS states service characteristics include items such as availability, performance, reliability, scalability, and vendor reliability (Kundra, 2011). This is not an all-inclusive list as each agency will have its own priorities for services that are migrated to the cloud.

The FCCS points out market characteristics are items such as the competitive nature and maturity of cloud services as it relates to the program (Kundra, 2011). Agencies should consider these factors to ensure the agency does not get into a one-sided agreement for cloud services that have yet to properly mature.

Kundra offers that network infrastructure refers to the government provided network (Kundra, 2011). The cloud is a service that is delivered over the use of the internet. Agencies need to ensure that the network provided to the end user is sufficient for the agency to properly access the cloud at will. If the agencies network has excessive downtimes then the program may not be a good candidate for cloud computing.

The FCCS discusses government readiness as the technical ability of the government to migrate a program to the cloud (Kundra, 2011). Questions that should be asked by the agency are do we have capable managers to oversee the migration and data stored in the cloud, do we have the technical expertise to negotiate a contract and applicable agreements, and does our organizations management tend to accept change.

Kundra further discusses the technology life cycle, which is simply where the current technology utilized is in its life cycle (Kundra, 2011). If the technology is relatively young with contracts that will incur significant costs to terminate then that program may not be a good candidate for cloud migration. Conversely, programs that are at the end of their life cycles and are requiring a tech refresh may be great candidates to migrate to the cloud.

The FCCS explores provisioning the cloud, which refers to effectively moving to a contract system of quality of service instead of number of server or bandwidth provided. Agencies that effectively migrate to the cloud excel in factors such as aggregating demand,

integrating services, contracting effectively, and realizing value. Aggregating demand means the agency should look at increasing their purchasing power by utilizing partnerships with other government organizations. Integrating services simply refers to ensuring that the cloud application is evaluated periodically to ensure that the system is remaining interoperable. Kundra indicates that contracting effectively is essential ensuring that the cloud system is setup to succeed through a proper contract. The contract should prevent a situation where only one vendor can meet the needs of the end user. In addition, service level agreements need to clearly spell out security requirements, performance requirements, and a continuity of operation plan. The metrics in the contract need to be concise to prevent the vendor and government having disagreements on the terms and conditions of the contract. Finally, the FCCS discusses realizing value which refers to the governments need to fully support the program once it is migrated to the cloud. Legacy systems should cease to exist and their assets either decommissioned or moved to support higher priority programs

Kundra further asserts, when a government organization migrates to a cloud-based application they must ensure that they are properly managing the contract (Kundra, 2011). This means that the government acquisition teams must change their mindset to acquiring services rather than the traditional mindset of acquiring assets. As such the government needs to ensure that they are actively monitoring the performance of the contract. This means staying on top of the terms and conditions and the service level agreements that are spelled out in the contract. If this is followed out properly by the government acquisition team there is no reason that a migration to the cloud would be difficult.

In 2017, the government expanded upon the Cloud First policy with the Cloud Smart policy. Cloud Smart instills that there are three factors that must be considered when considering cloud computing. These factors are security, procurement, and workforce. Cloud Smart provides guidance on how to consider these factors when sourcing cloud computing. Cloud Smart keeps much of the NIST definition of a cloud but explains that the more the cloud gets utilized the blurrier the lines between a true IaaS, PaaS, and SaaS become. In this instance most clouds are becoming more of a hybrid cloud due to the need to meet customer demands. Lastly, Cloud Smart realizes that modernizing by moving to

the cloud is not a one-time process that suddenly makes technology modern. Agencies must continually evaluate their processes to stay modern.

With regard to security, Cloud Smart instructs agencies to take a risk-based approach to securing the cloud environment (Chief Information Officers Council, n.d.). To assist in reducing the risk, Cloud Smart requires an emphasis on "defense-in-depth," which is having protections at the data layer, network infrastructure layer, and physical infrastructure layer (Chief Information Officers Council, n.d.). In order to manage risks, Cloud Smart encourages the utilization of Service Level Agreements (SLA) with the cloud service provider. These SLAs should provide clear roles in the protection of data to include required notifications when that data is compromised. "Cloud Smart encourages agencies to approach security in terms of intended outcomes and capabilities" (Chief Information Officers Council, n.d., Section II, Paragraph 4). This is similar to how the government procures many commodities and services at the operational level and allows the industry to utilize breakthroughs in an expedient manner. This allows the government's data security to keep up with the industry.

Cloud Smart addresses the issue with the procurement of cloud services. One of the main issues is that many services that may not be marketed as cloud services still require information to be passed through or stored on a cloud-based systems (Chief Information Officers Council, n.d.). This creates both security and privacy concerns as this data may not be required to be protected as well as it should. To address security issues, agencies should utilize SLAs and pay attention to the Federal CIO High Value Asset (HVA) memorandum. In addition, to reduce costs, agencies should consider category management when procuring cloud services.

Cloud Smart developed what is referred to as a two-track approach for SLAs in the procurement of cloud-based services. "The first track of activities to support the effective use of SLAs involve the government-wide review and selection of contractual terms and conditions" (Chief Information Officers Council, n.d., Section III, Paragraph 7). The result of this approach is to come to a standardized SLA to help provide a more efficient and secure cloud service (Chief Information Officers Council, n.d.). The second track is facilitating risk management through well-established "roles and responsibilities, establish

clear performance metrics, and implement remediation plans for non-compliance" (Chief Information Officers Council, n.d.. Section III, Paragraph 8). This allows "agencies a way to mitigate risk while optimizing the performance and efficiency of their newly procured cloud-based solution." (Chief Information Officers Council, n.d.).

The final items touched on by Cloud Smart is the federal workforce support cloud computing (Chief Information Officers Council, n.d.). Cloud Smart calls for agencies to identify skill gaps in work roles particularly those IT professionals that are instrumental to the implementation of cloud-based services. Once those gaps are identified agencies should make it a priority to reskill employees that may need additional training. In addition, federal agencies need to make a concerted effort to retain employees that have the necessary skills and put them in positions where they can affect cloud-based services. Lastly, if the federal agency cannot reskill or retain the skills necessary for successful migration and utilization of cloud-based services they will need to recruit and hire employees to address these skill gaps.

F. METHODS OF GOVERNMENT CONTRACT STORAGE

Throughout the history of DoDEA and USAF the main method of contract storage has been storing physical paper copies. With the policies of the late 1990s to institute digital environments and create a paperless contracting process the DOD greatly reduced both the procurement time and paper waste generated in the contracting process. (Sherman & Freeman, 2007). And while the DOD has made big strides since the days of hand-delivered requirement packages, many units struggle to adapt to the changes with technology in the workplace. With this policy, DOD contracting moved to modernize the workforce's tools through systems such as Standard Procurement System, DEAMS, and contract writing systems such as PD2 and CONWRITE. These new systems clearly upgraded the old systems allowing for quicker procurements and changes when needed. These upgrades were focused on reducing the time spent generating requirements and the paper required to submit a requirement. The upgrades also focused on the contracting documents generation process. Despite these modernizations, offices still resorted to printing out hard copies of the entire contract files and storing them in binders instead of utilizing electronic storage.

As time and technology progressed, offices slowly began migrating their contract storage to local shared drives or local electronic record management drives. This has greatly improved the ability of contracting offices to search for data within their own office, it still limits each contracting professional access to only their local offices files. While this was the status quo for many years a recent push has led to an upgrade of both contract generation and contract storage systems. In USAF, contracting leadership is rolling out CON-IT for contract generation and KT File Share for contract storage. These systems will be explained in Chapter III—Current Storage Systems.

G. CURRENT STATE OF THE ART IN THE COMMERCIAL SECTOR

At the moment cloud computing is the near past, present, and seemingly the future of computing in one form or another. It is anticipated that in the near future we will see an evolution in the method of cloud computing. This is due to the impracticability of having server farms process the data that will be generated in the very near future. It is estimated that the number of devices connected to the internet will increase to 27.1 billion in 2021 compared to 17.1 billion in 2016 and data generated will increase to 847 ZB from 218 Zettabyte (ZB) in 2016 (Wang, 2019). As the amount of data that is stored in the cloud increase so must the server farms that are keeping this data. As those server farms increase storage they also need to increase both the physical space and power consumption of each server farm. This method of exponential increase in space and power then becomes unsustainable as there is both limited space and power. Due to these limitations the tech industry has been working on different methods of mitigation.

One such emerging technology is called edge computing (Wang, 2019). While the idea of edge computing can be traced all the back to AKMAAI and IBM in 2003 its actual application is fairly new (Wang, 2019). To understand the edge computing you must first understand there are three layers of cloud computing. The first layer is the ending layer which consists of the user devices such as computers, smartphones, smart vehicles, etc. (Wang, 2019). The second layer is the edge computing layer which resides at the edge of the network and consists of devices such as network devices and edge servers (Wang, 2019). The third and final layer is the cloud layer which consists of the servers and storage

devices that make up the cloud (Wang, 2019). Simplified edge computing is taking many of the calculations that are completed at the cloud level and moving them to the edge computing layer (Wang, 2019). This allows for reduced amount of traffic to the cloud as only the necessary information is then passed to the cloud layer for processing and storage. It is believed that by utilizing edge computing, end users will see better real-time data processing and analysis, easier methods to protect personal data, easier scalability, increased location awareness, and a reduced flow of data (Wang, 2019). Additionally, it is possible that security can be increased through edge computing due to the fact that there is no longer a single point of failure in the system (Wang, 2019). Currently, if all data is stored at one cloud location all that data is vulnerable to a power outage. It is worth noting that other scholars believe that edge computing is actually less secure. In their thesis, Next Generation Cloud Computing, Varghese and Buyya argue that having a wide range of nodes that are accessible increases the opportunities for a malicious actor to compromise the network (Varghese & Buyya, 2017). They do, however, also see many of the same benefits that were stated earlier including an increased quality of service and experience due to reduce latencies (Varghese & Buyya, 2017).

The idea of a multi-cloud has been around for a while but has recently seen an increase in usage (Varghese & Buyya, 2017). The essentials of a multi-cloud are to utilize resources of multiple data centers, thus reducing the burden on one center (Varghese & Buyya, 2017). This method does come with some issue chiefly the interconnectibility between multiple different architectures are the cloud level (Varghese & Buyya, 2017). To combat this issue there are two types of multi-clouds that should be considered, the hybrid cloud and the federated cloud. A hybrid cloud is simply combing public and private clouds and infrastructure (Varghese & Buyya, 2017). Since both private and public resources are being utilized, it can be beneficial to utilize when dealing with sensitive data as all the sensitive data can be kept on the private servers. The network can be a major concern when utilizing a hybrid cloud as items such as bandwidth and latency need to be considered for access from private clouds to public clouds (Varghese & Buyya, 2017). This issue could be resolved with dedicated networking but that requires additional asset management on the private server side (Varghese & Buyya, 2017). A federated cloud is bringing multiple

cloud providers under one agreement to utilize the same architecture (Varghese & Buyya, 2017). This solves many issues such as interconnectibility issues since data can easily be transferred from one provider to another (Varghese & Buyya, 2017). While there are many examples of this happening around the world, it is usually a joint effort by smaller cloud providers as larger providers with global reaches are less inclined to federate their resources (Varghese & Buyya, 2017).

Currently, there is also the exploration of creating heterogeneous clouds. One of the main issues with cloud computing is compatibility with the software that is being run at the cloud server level. A heterogeneous cloud seeks to solve that issue by utilizing different types of processors at the cloud level to allow the end user to run any machine they wish (Varghese & Buyya, 2017). Heterogeneous clouds are in development but could be seen in the near future, based on the growth rate within the industry. The biggest current issue with heterogeneous clouds is programmer's current inability to write code that is oblivious to the architecture on which it is being run (Varghese & Buyya, 2017).

The commercial marketplace is also looking into changing the architectures within the clouds. Some of the emerging architectures are serverless computing and software-defining computing. Despite its name serverless computing is not in fact serverless (Varghese & Buyya, 2017). This process is actually an update in the pricing structure that traditional clouds utilize. With the understanding that more devices are going to edge computing, serverless computing would result in the end user only being charged for the functions utilized on the cloud (Varghese & Buyya, 2017). This is opposite of what currently happens when an end user essentially "rents" a virtual machine full time whether it is used or not (Varghese & Buyya, 2017). This model relies on many processes to be completed at the edge and therefore you only pay for what you use. Lastly, software-defining computing is an approach that is being explored to better help the network flow between multiple servers. The approach is attempting to isolate the underlying hardware in the network from the components that control data traffic (Varghese & Buyya, 2017, p. 9). The end goal is to ease configuring and operating of the infrastructure to assist in increasing the quality of service (Varghese & Buyya, 2017).

H. CONCLUSION

This chapter served to introduce the reader to the essence of cloud computing and explained conceptual models, designs and functionalities as well as advantages and disadvantages of utilizing cloud storage for government contract documentation. It also provided key aspects of the current government policy on Cloud Computing in relation to an historic perspective on government contract storage.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CURRENT SYSTEMS

A. INTRODUCTION

This chapter serves to discuss the current government contract documentation storage systems in place as well as contrast them with the current commercial storage and data systems. In addition, this chapter includes a discussion of emerging technologies and trends in the Cloud Computing world. Much of the information in Chapters III and IV with regard to the current systems and pros and cons of those systems is generated utilizing the knowledge of the two writers as subject matter experts. Few if any scholarly articles are available for use so the experience working in the systems is utilized.

B. CURRENT GOVERNMENT SYSTEMS

Currently the DoDEA and USAF are utilizing multiple different systems for both contract generation and contract storage. Both organizations utilize Electronic Document Access (EDA) and KT File Share for some manner of contract document storage. In addition, both organizations utilize CON-IT as a method of contract writing. USAF has some additional contract generation systems that include CONWRITE and PD2. USAF units operating out of KT File Share utilize either electronic records management (ERM) drive or shared drive storage from servers located on-site. Lastly, some USAF units still utilize paper copies of contracts that are stored in filing cabinet or on desks as the primary storage of contracts.

C. CONTRACT STORAGE

In USAF, EDA is primarily used to store contracts themselves and any modifications. This information is relayed to the Defense Finance and Accounting Services to be obligated for payment when a valid invoice is submitted and accepted in the IRAPT module of Wide Area Workflow. Documents stored are limited to documents that are meant to obligate or de-obligate money, such as, purchase orders, delivery orders, task orders, and modifications. Users who have access to this system can review any contractual document that is loaded, regardless of organization, as long as the user has the contract

number. When combined with the USAF market research system EZQuery, EDA becomes a very useful tool. EZQuery allows users to search contracts based on contracting office, description, vendor, among many other search criteria over a set period of time. Users then get a list of contracts that match the search criteria. Users can than utilize the contract numbers in EDA to search for the contractual documents to which they want access. With this the user gets access to the actual contract which can be useful when comparing pricing, generating market research reports, or determining potential set-asides. For contracting professionals this is as useful as EDA is for contract sharing.

KT FileShare is a SharePoint based contract filing system that is slowly being implemented throughout the USAF and DoDEA as the primary method of contract storage. The goal of KT FileShare is to replace antiquated paper storage methods and locally based server storage systems. When a contract file is started in KT FileShare the user starts a contract documentation coversheet where the user fills in information such as the contract/ solicitation procurement instrument identifier, estimated contract amount, simplified acquisition, commercial item, and contract type. A contract file is then generated from these answers with the programs suggested folders. The user can then choose to delete or add different folders as they see fit to meet the needs of their specific acquisition. In addition, users can create a template contract file folder structures from previously created file folders. This allows users to expedite creating a contract file on the front end. Each folder within KT FileShare then allows users to upload documents such as purchase requests, market research reports, and contracts into the individual folders to create finalized contract files. The files within each folder can also be sent to reviewers for edits and signature, which all can be done within this system. Overall, the system is fairly intuitive and allows for a more standardized filing system across the USAF and DoDEA.

Each contracting office is segmented within KT FileShare to only see their own contract files. KT FileShare users can utilize a filter feature within the system to sort or search the contract files that are assigned to them or contract files assigned to their contracting office. Currently, KT FileShare does not allow users to search for or access files that are not within their own contracting office. In addition, users cannot add or delete documents from a contract folder if they are not provided permissions to be assigned to

access, view and post content to it as a contract administrator or contracting officer. If neither assigned administrators nor contracting officers are available then a site user administrator has to go in and assign a new contract administrator or contracting officer to the contract file. This process causes a situation where leave, PCS, and deployment can cause a file to become unusable if appropriate alternates are not assigned to each contract file. Despite these potential flaws, KT File Share does well at standardizing contract files across many different bases.

KT FileShare allows users to assign any person that is found in the USAF global address book as a contract reader. This assists contracting offices with items such as higher headquarter reviews and legal reviews. These contract readers are allowed to add documents to folders within KT FileShare which allows for legal reviews and clearance reviews to be completed within KT FileShare. This makes KT FileShare a very useful tool for higher headquarter organizations when contract reviews are necessary.

Many USAF contracting offices continue to utilize on-site servers as the primary storage method for their contract files. When an on-site server is utilized any person that knows the path or is granted access to the server path can edit, add, and delete files within the server. Contracting offices that utilize on-site servers tend to have template folders created to a variety of different types of acquisitions to include simplified acquisition contracts, multi-year services, and construction contracts. The reason different templates are utilized is simply because each type of contracting file has different documents that are required. Users utilize programs from the Microsoft office suite (Word, Excel, PowerPoint, etc.) to create each document for the folder and then save them in the appropriate folder much like anyone saves a file on their computer. Any contract administrator or contracting officer or person in general that has access to this file path can add, delete, and edit any document that another user place in the folder. This reduces the risk of a contract administrator or contracting officer going on leave, PCS'ing, or deploying and rendering a file unusable. However, this structure also limits a user's search capability to what is on that server.

If there were an agreement in place between multiple contracting offices then, theoretically, access to all files belonging to any of those organizations could be accessed.

This in itself may result in a security concern as an indefinite amount of people would be able to access files they may not otherwise have access. However, the benefits gained from that access may outweigh the risk.

Some contracting offices are still utilizing filing cabinets to store paper copies of contracts with no electronic presence. Contract administrators utilize Microsoft Office suite products to create documents and print them out and put them in a physical contract file for storage. While this is an inconvenient method of storage for retrieving files and documents alike, it is the most secure method of contract storage. In order to steal contract data, one must gain physical access to the building that the filing cabinet is stored and then gain access to the filing cabinet. As many federal contracting offices are located in secure buildings that are locked and guarded at night it becomes an impracticality to steal the files. The large downfalls of this method of storage is the paper waste generated by fully printing all documentation of a contract folder, the large amount of physical storage space necessary to house the cabinets, and the lack of ease of locating and sharing contract documents.

D. CONTRACT WRITING

Currently the primary method of delivering contract writing systems is through on-site servers. Two samples of these systems are PD2 and CONWRITE. While there are many more programs than just these two, they all share the same characteristics. These contract writing systems are programs that run off servers that are normally located at the contracting offices' location. These systems' primary purpose is the generation of contracting documents such are Standard Form (SF) 1449 (purchase order, delivery order, solicitation, etc.), SF 30 (modifications and amendments), SF 1442 (construction contracts), and other such documents. On-site systems have cabinets or folder systems that allow for the storage of generated documents as well as the ability to upload attachments to the contractual documents. The uploads tend to be limited to documents that affect the solicitation or contract itself such as performance work statements, statement of works, and wage determinations. Contract documents such as determination and findings, justification and approvals, price negotiation memorandums, and price fair and reasonable determinations are not uploaded into these systems creating an incomplete contract file.

The Air Force recently began implementing a contract writing system called CON-IT which is a cloud-based contract writing system accessed over the internet. This system is in its infancy and offers fewer contracting functions than its predecessors. As it is currently implemented, CON-IT allows the generation and storage of contract documents such as Standard Forms (SF) 1449, SF 1442, and SF 30. One glaring feature that is missing from CON-IT is the ability to generate Department of Defense (DD) Form 1594 and DD Form 1597 which are crucial and mandatory reporting documents for contract closeout. In addition, contracts cannot be closed out in the system at this time. The development team for CON-IT are continuously working to update the systems with more features to make it more user-friendly and more inclusive to the contracting process.

E. CURRENT COMMERCIAL SYSTEMS

Rapid growth for information technology services has led to an increase in infrastructure needs ranging from navigating industry failures in data centers themselves to a need for more businesses that require continuity of data processing operations (ESDS, 2010). Several types of approaches have presented themselves in the marketplace commercial industries can choose from to resolve their requirements as follows:

1. Different Types of Commercial Data Centers and Their Different Tasks

ESDS lists four separate data centers that can be used for certain business models and have their own operation problems:

- Corporate data centers
- Web hosting data centers, providing computer infrastructure as a service (IaaS)
- Data centers that provide TurnKey Solutions
- Data centers (portals) that use the technology to Web 2.0. (ESDS, 2010, Paragraph 3)

Along with the type of data center, there are some considerations that must be taken into account that significantly affects the type of data center that is chosen. These considerations are:

- Bandwidth type (internal, external or mixed)

- The use of Layer 2 (L2) and/or Layer 3 (L3) for traffic control at the center of the periphery or top of the rack
- Data Storage Technology
- Level of server virtualization
- Overall size of the data center (number of servers). (ESDS, 2010, Paragraph 3)

The blog entry by ESDS explores different types of data centers and how they are utilized (ESDS, 2010). The data centers can range from 200 to over 1000 server and are designed to optimize applications and services. ESDS indicates very few of these include the necessary technology for scientific analysis. Lastly, a large amount are designed for customer service.

2. Development of Corporate Data Centers

ESDS indicates that there are two prevalent trends for data centers (ESDS, 2010). These two trends are, "use of server virtualization technologies that make more efficient use of hardware resources, and the transition to mixed networks that combine LAN Technology-based Ethernet, and fiber-optic network storage or SAN." (para 5). ESDS discusses the development of "turn-key data centers" which are essentially data centers that provide a space for clients with immediate needs.

3. Internet Hosting

Lastly, ESDS discusses the features of internet hosting (ESDS, 2010). ESDS explains that all types of firms provide hosting services. Their key to survival in this business is being versatile in meeting the demands of their clients. ESDS explains that the need for these services have increased because advancements in virtualization technologies.

4. Data Center Lessons

In her book, *Managing Chaos, Digital Governance by Design,* Lisa Welchman states that there are digital governance problems that lead to complicated outcomes. Power struggles with the advent of the World-Wide Web and Internet, manifest themselves publicly 24 hours a day, 7 days a week. That said, the very nature of the term digital

development exudes complexity—complexity in delivery and complexity in the teams and systems that innovate, develop and manage digital functionality. Rather than a simple approach, she advocates for calming and clarifying roles and responsibilities of digital development. Therefore, "cloud computing has the potential to significantly influence the outsourcing decision. As cloud computing matures, application development and delivery may become more cost effective in the cloud than in the data center and more cost effective than colocation and managed hosting." (TechTarget, 2010, Pg. 4). As such, the concept of digital governance demands that technology becomes not only a driver of more diverse service channels for more sophisticated and advanced users, but also a platform for expanding participative capacities for all public citizens. This last statement speaks to what cloud computing deployment models agencies should select be it a cloud-based application, a hybrid or on-premises.

5. Current Commercial Service Providers in the Marketplace

Power players that have already developed commercial cloud applications for the commercial marketplace and have now honed cloud applications for the federal government are Amazon and Google, in addition to many others. Amazon's version is called AWS GovCloud while Goggle's is called Gsuite and Google Cloud Platform and Products. An online resource site called the "Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services." "It is a unique government program that focuses on cloud technology, cybersecurity and risk management. FedRAMP provides a standardized framework to security assessment, authorization, and continuous monitoring for cloud products and services." Once at the FedRAMP site, a user can navigate to the marketplace (https://marketplace.fedramp.gov) to see the array of cloud providers, what service models they offer and the assessment that the site has provided from a security authorization prospective.

F. GOVERNMENT CONSIDERATIONS AND TRENDS

Based on a VAO article titled, "Cloud Spending and Savings Are Up in the Air," cloud adoption is on the rise in federal agencies, yet there still remains scant data on related spending and savings limits with which to make sound informed acquisition decisions (GAO) (Virtual Acquisition Office, 2019a). Of the 16 agencies GAO reviewed, 11 percent stated that their fiscal year (FY) 2019 IT investments will likely be used for cloud services, an increase of 3 percent from FY2016 (Virtual Acquisition Office, 2019a). In addition, the same 16 agencies reported an increase in cloud spending in order to reap cost savings, yet the data presented for the GAOs review is incomplete (Virtual Acquisition Office, 2019a). The agencies cite inconsistent processes for tracking spending and savings on cloud costs (Virtual Acquisition Office, 2019a). Overall, the 16 agencies found "significant benefits" with their procurement of cloud services, such as improved customer service and more cost-effective IT infrastructure and service management options (Virtual Acquisition Office, 2019a). Complicating matters is the fact that any government cloud contract is now being seen as possibly being done without a bid. The VAO article "How Microsoft Could Win an $8B Cloud Contract without a Bid," describes the fact that the tech giant Microsoft with its $8 billion dollars Defense Enterprise Office Solution (DEOS) contract is tough to beat in the realm of cloud-based business tools for the public sector (Virtual Acquistion Office, 2019b). Furthermore, it is stated that, "Microsoft is the only company that has the capabilities the Pentagon is requesting, and is already widely used across the Department of Defense and has the security certifications to handle sensitive military data." (Virtual Acquistion Office, 2019b). Since FY2015, Microsoft has taken home roughly $4.2 billion through software licensing agreements with federal agencies (Virtual Acquistion Office, 2019b). By comparison, Google, its closest competitor has captured only $97 million with its G Suite during the same timeframe (Virtual Acquistion Office, 2019b). It would also take Google and any other would-be competitors' years to meet DEOS' impact levels 5 and 6 security requirements though Microsoft could potentially qualify within the year (Virtual Acquistion Office, 2019b). What is currently trending in 2019 and 2020 are Hybrid Clouds which the government officials expect to see a bigger emphasis on based on the flexibility of hybrid cloud infrastructure, and because of the need for legacy applications

which are not built for the cloud, FedScoop reports (Virtual Acquisiton Office, 2018). In fact, 2019 was heralded by IT industry experts as the "Year of the Hybrid Cloud." A hybrid cloud system has the advantage of being a "composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)".

Many factors can affect agencies cloud migration and cloud procurement decision-making including cloud providers' compliance with the FedRAMP guidelines or Defense Information Systems Agency (DISA) security requirements (Virtual Acquistion Office, 2016). Currently, government agencies are leaning to the software-as-a-service (SaaS) cloud computing model due in part to the policy guidance that has been forwarded down from the Office of Management and Budget (OMB). In their Federal Cloud Computer Strategy, the CIO for OMB states that the Cloud Computing Strategy will be "Cloud Smart" which "is a long-term high-level strategy to drive cloud adoption in Federal agencies." (From cloud first to cloud smart, n.d., para 2). "Cloud Smart focuses on three inter-related areas to drive cloud adoption through building knowledge in government and removing burdensome policy barriers (Policies & priorities cloud smart, n.d., para 3)." The three focus areas are Security, Workforce and Procurement (Chief Information Officers Council, n.d.). All three are to work in tandem to drive IT cloud savings, improve security and deliver mission-serving solutions faster. OMB's IT guidance also is recommending that Federal agencies move from redefining IT from an asset to a service. They cite the Defense Information System Agency (DISA) Rapid Access Computing Environment (RACE) that has taken IT infrastructure from an asset management function to a service provisioning function.

G. CONCLUSION

This chapter provides a conceptual overview of the present-day government data storage systems and gives the framework for what commercial data storage systems and service providers exist in the current industry marketplace. Along with a discussion of

cloud computing trends, this chapter served to provide factors bearing consideration in cloud procurement decision-making for procurement data storage.

IV. ANALYSIS

A. INTRODUCTION

This chapter serves to provide the strengths and weaknesses of the current government procurement data storage systems as well as conduct further analysis based on the researchers' findings for the feasibility of government cloud computing for data storage. The chapter closes on what improvements the government can make in this area for more efficient contract documentation preservation and security.

B. STRENGTHS AND WEAKNESSES OF CURRENT GOVERNMENT SYSTEMS

Table 1 summarizes the strengths and weaknesses of the EDA document storage system. The EDA document storage system would be considered a community cloud on a private server. Government users can request and gain access through the Wide Area Workflow Portal. Authorized users can access the system with their government issued common access card (CAC) from any location where they have internet access and have their computer set-up with a VPN. All users that are granted access can utilize this system to search for contracts awarded at DOD contracting offices as long as the contract number is known. This limits the abilities of the end user to find other contracts easily since other systems need to be utilized to find the contract numbers.

EDA is a mature system within DOD contracting and financial communities. This makes it a known commodity that users are very comfortable with and understand. In addition, its length of service has increased the chances that security flaws within the programming itself have been found and corrected reducing security threats associated with the system. Additionally, a majority of the files stored within EDA are or should be public knowledge so the risk associated with a data breach of information in EDA is low.

EDA severely limits the end user in files that can be stored. Currently, the contracting community utilizes the system to upload all contracts and subsequent modifications. DFAS utilizes the information from EDA to obligate the funds loaded onto a contract. EDA does not allow user to upload any other contractual information such as

market research, determination and findings, and justifications and approvals. Overall, the systems are very useful if the contract number is known and all that is needed is information that is on the contract or a modification.

Table 1. EDA Strengths and Weaknesses

Strengths	**Weaknesses**
Secure System	Limited Storage Capability
Mature System—Known Commodity	Rigid Storage System
Cloud Based—Access Anywhere	

Table 2 summarizes the strengths and weaknesses of the KT FileShare contract storage system. KT FileShare is a SharePoint based contract storage system that allows authorized users to access the system from anywhere with a CAC and internet access.

KT FileShare is also a system that is in its infant stage of deployment. As a young system, KT FileShare gets regular upgrades and that change the user experience. Each update is an attempt to improve the efficiency and usefulness of the program. However, just like any system updates can cause unintended interruptions in user access or unintended security flaws. One such case made the system un-accessible for approximately two weeks while a subsequent upgrade was developed to fix the issue.

KT FileShare was specifically developed for contract file storage which allows for a certain degree of flexibility. Users can pick and choose the contract file folders they would like to have included into a specific contract and then add files to each individual folder. Each folder falls under one of seven separate categories (requirements, pre-solicitation, solicitation, pre-award, award, contract administration, and pending close-out) which relate to a stage in the contract life cycle. These file structures fall in-line with what leadership deems essential for a contract file. Since access can be granted to anyone with a CAC KT FileShare allows for remote inspections of contract files for higher headquarter reviews and inspections. This helps expedite these processes and will help reduce

temporary duty costs for inspectors that are normally sent to different locations to inspect files.

Currently, access is granted at an office level within KT FileShare which limits users to only be able to search files that have completed in the office they are assigned. This is very helpful because you have full access to files within that office and are free to read any contractual documents that are not considered sensitive. Documents that are considered source selection documents can only be read by the contracting officer, contract administrator, and anyone that is given source selection reader access to the file. Other than those specific files administrators can view market research documents, price fair and reasonable determinations, justification and approvals, etc. These documents are very helpful since it gives contracting professionals background information on how a contract was previously purchased.

While this is very helpful it is still very limiting since documents are limited to those within a certain office. If this could be opened up to allow even view only access to other offices files the contracting career field would benefit greatly. Contracting professionals could then research how other offices have procured commodities, services, and construction and may find a better way to compete their own requirements.

Table 2. KT FileShare Strengths and Weaknesses

Strengths	**Weaknesses**
Flexible Storage Capability	Infant System
Cloud Based—Access Anywhere	Internet Can Limit Access

Table 3 summarizes the strengths and weaknesses of utilizing the physical storage method for contracts. The main strength of a paper or physical storage is that it is very easy to secure the file from unwanted access. In order to access a physically stored file a person would first have to gain access to the facility that the file is stored. Then depending on the storage method, the contract file would need to be found either in a filing cabinet or

on a person's desk. Since an adversary would need to be physically at the site to gain access to the file, they would need to gain access to the facility when no persons were present on site. They would also have to spend time searching through any number of files to find the file that they would need. This leads to the highest risk in paper storage is the actual contracting professionals themselves. If compromised a contracting professional could give adversaries access to numerous files, they would otherwise not have been able to gain access.

In order for a contracting professional to gain access to a paper file at another location they would have to contact a point of contact at that location with the contract number and documents for which they are looking. Then it is left to hoping that the file in question can be located and the documents that are needed actually got filed. In addition, the person at the location would have to be willing to scan all the requested documents and email them to the contracting professional.

Lastly, paper storage has a weakness that other storage methods do not have and that is physically limited space. An office can only store as many files for which they have physical space. Once they run out of space "in-house" they have to send older files to a staging area that could be anywhere from down the street to in a different city or even state. This extremely limits the ability of a contracting office to access even their own files.

Table 3. Paper Storage Strengths and Weaknesses

Strengths	**Weaknesses**
Extremely Secure System	Limited Storage Capability
	Limited Access—Physical Location

Table 4 summarizes the strengths and weaknesses of the PD2 contract writing system. PD2 is not a cloud-based system but is a private server based contracting program that can only be accessed by a connection via a local area network (LAN). As such this provides enhanced security as the local client service administrator (CSA) can control who

and what devices have access to that LAN. Usually, these LANs are protected from hacking but as an extra layer of security government networks are also protected against unauthorized users. The biggest threat to unauthorized access is a user within the system downloading and sharing data to adversaries. However, that user would be limited to documents at their site reducing the risk of an agency wide incursion.

PD2 is a mature system for contract writing. As such most of the technical issues with the system have already been resolved. Any new issues that arise in the system tend to be due to new external systems being created that need to interface with the system. However, to keep with new technological advancements, PD2 also requires constant updates to maintain the systems integrity with the new hardware and software. This process requires many labor hours on behalf of the contractor to write the new codes for the update as well as man hours needed to troubleshoot any field issues that arise from the update. In addition, the end users experience demand for additional man hours for the client service administrators to apply the updates at the server level for the program.

Lastly, the main issue with PD2 is that end users must have access the LAN in order to access this system. This means users must be on-site to work on contract files in the system limiting the ability to work from anywhere.

Table 4. PD2 Strengths and Weaknesses

Strengths	**Weaknesses**
Secure and difficult to breach	Antiquated
Single Malicious User Limited to One Site	Time Consuming to Update
Mature System—Known Commodity	Limited Access—LAN
	Document Generation Only

Table 5 summarizes the strengths and weaknesses of the CON-IT contract writing system. CON-IT is the newest iteration of contract writing within the Air Force and DoDEA. The system is a cloud-based system that allows authorized users to access the system anywhere they have an internet connection and a VPN. This allows for contracting professionals to telework when it is necessary. In addition, it allows a contracting office to change sites with minimal down time if something happens to their physical office. However, since it is cloud based and requires an internet connection to run it is vulnerable to network outages. Therefore, if the network is down, there is no way to access the system requiring users to manually create any contracting documents.

Although CON-IT was created off of the system that is currently utilized by the USDA it has been modified for the needs of USAF and DoDEA. Since this is the case, the system is very new and requires updates regularly to increase the functionality of the system. These updates are essential in not only increasing the functionality of the system but to fix bugs that exist within the system. When CON-IT was first released to USAF it experienced large connectivity issues due to the systems being too stressed. Although, this has seemed to be fixed it is a risk to happen again whenever there are too many concurrent users.

CON-IT is currently only utilized for contract document generation meaning only contracts and modifications can be completed and stored in the system. However, the system does have the beginning infrastructure of a complete storage solution for contracts. Since this not an official capacity of the system, users does not utilize it for documents outside of attachments to the contract such as statements of work, performance work statements, or wage determinations.

CON-IT's development was completed with DISA requirements in mind. The system currently meets DISA requirements for being a cloud-based service. While this is a positive for the system it does have some unintended negative impacts that need to be addressed. Mainly the system requires users to be forcibly logged out after 5 minutes of inactivity. While this may be a minor inconvenience it becomes very problematic when you are working on a contract document and get a phone call that lasts more than 5 minutes. In this case all the work that was completed on the current page is lost. To circumvent this

issue end users must ensure that they are advancing the screen anytime they may be away for more than 5 minutes.

Lastly, CON-IT interfaces with the Clause Logic System (CLS) that is located on the WAWF Suite. This system is run by Defense Pricing and Contracting (DPC) which are the experts on clauses. CLS requires the user to answer multiple choice type questions and based on the answer selects the clauses that are required for a contract action. All the questions and clause sets have been vetted by DPC and are considered legally sufficient for contracting actions. This reduces the risks of missing key clauses but also makes contract specialists reliant on a system instead of their knowledge and skills.

Table 5. CON-IT Strengths Weaknesses

Strengths	**Weaknesses**
Cloud Based—Access Anywhere	Infant System
Meets DISA Requirements	Network Can Limit Access
Clauses Loaded Based on DPC Algorithm	Document Generation Only

C. WHERE IMPROVEMENTS CAN BE MADE

The government is primarily utilizing two separate systems, CON-IT for contract writing and KT FileShare for contract storage. Both systems have their flaws which need to be addressed in order to make a rock-solid system. The main flaw is the fact that there are at least two systems that contract specialists need to utilize in order to create and store contracts. This leads to potential continuity problems in contract files as the completion of the file is reliant upon contract specialists to download the final contract from one system and upload it in another. In addition, all other documents need to be generated outside both systems in programs such as Microsoft Word, Microsoft Excel, or Adobe. This leads to an increased chance that key contract documents can be misplaced or not loaded at all. If these two systems are going to be the future of USAF and DoDEA contracting than efforts need

to be made to reduce the chances of documents not making it into the contract file. Options to consider could and should include:

An automatic "behind the scenes" interface between CON-IT and KT FileShare. This interface could automatically transfer a signed contract, signed modifications, and completed Contract Action Reports (CAR) from CON-IT to KT FileShare.

Incorporating office level templates and allowing document generation in KT FileShare. If contracting offices could upload agency specific template files in KT FileShare and KT FileShare allowed contract specialists to create documents within the system then fewer documents would be created outside the systems. This would effectively reduce the chances of files not being uploaded into the official contract file. An additional necessity for this to work would be the ability to convert documents to a PDF in the system, which would allow for digital signatures.

Another option to consider would be to expand upon CON-IT's inherent storage system and make it the official contract storage system. This would completely eliminate the dual system approach and ensure at a minimum all signed contracts, modifications, and completed CAR's would be in the contract file. This would then require the contract specialist to upload all other documents to just CON-IT.

Another area that could be improved upon is the connectivity issue. Whenever the government network goes down it drastically slows the contracting process for those offices utilizing CON-IT and KT FileShare. As web-based or network-based systems both are reliant on the network being in working order. When the network goes down no work can be completed in either system. This forces contract specialists to either wait for the network to return to operational status or start completing manual contract actions. As it stands, a manual action cannot be uploaded into the system, so if a manual action were completed, a contract specialist would then be required to create the action in CON-IT after the fact and upload the manual version as the signed copy. This leads to inconsistencies in the official contract file and what was actually completed. This is a tough issue to solve since having multiple systems would be an expensive redundancy. However, one redundancy that may not be terribly expensive for office use would be to acquire

commercial Wi-Fi or hotspots for contracting offices. With the increased usage of laptops, contract specialists could utilize a VPN and access the systems while the government network is offline. Other workarounds could include a redundant storage system automatically uploading all contracts to a server on-site that can be accessed when the network is down. While this doesn't allow for the creation of contracts easily it allows contract specialists to view contracts and make decisions on contract issues.

The final recommended improvement would be to interconnect all contracting offices. This function would be useful but only utilized as a search and read-only function and not allow offices to edit other offices files. This would be immensely beneficial to all contract specialists as they would be able to see what other contracting offices were doing for the same or similar projects. To implement this, USAF and the DoDEA would have to decide on a contract storage system. Once that system is decided upon, a simple keyword search function could be added to allow a contract specialist to search for all documents or contracts containing that keyword. From there allowing read only access for all users to non-sensitive contracts would allow the contract specialist to look at a variety of contract documents to include market research, price negotiation memorandums, justifications and approvals, and determination and findings. This would be helpful since it would allow contract specialists to find practices that may be better than their offices practices or increase the accuracy of a market research report.

D. STRENGTHS AND WEAKNESSES OF CURRENT COMMERCIAL SYSTEMS

At the current moment there are three different vendors that have differentiated themselves from the competition in the commercial marketplace. These three vendors should be no surprise to anyone, Amazon with Amazon Web Services (AWS), Microsoft with Microsoft Azure, and Google with Google Cloud Platform (GPF). Unfortunately, due to the rapid changes in technologies in the cloud computing realm there are not many academic articles for these services. As such respected IT sites such as Varonis and ZDNet were utilized to get data to analyze the current commercial offerings.

1. Strengths and Weaknesses of AWS

As stated in Chapter II, Amazon was one of the first companies to explore utilizing the cloud for commercial gain with AWS in 2002. With this they have a clear cut advantage of age and experience in the realm of cloud-based enterprise solutions (Petters, 2020).

Table 6 provides a summary of Amazon's prime cloud-based offering called AWS. Amazon clearly pulls heavily on its vast experience and sheer size to dominate the commercial marketplace for cloud storage and applications. AWS Elastic Compute Cloud can be considered a "department store" of enterprise solutions in the cloud (Petters, 2020). This service gives the users plenty of options to choose from to make up for their lack of personalization (Petters, 2020).

In the storage realm AWS offers a wide range of options for both on and off premises storage (Petters, 2020). However, they do lose some abilities by providing very limited backup service options (Petters, 2020). Additionally, AWS does not provide a hybrid solution, forcing end users to utilize their server to create one (Petters, 2020). This may show that Amazon is not keeping up with the times as hybrid servers seem to be one of the main components that are looked at for future clouds.

AWS is truly at the head of the field when it comes to the tools they are providing. AWS is at the fore front of the market when it comes to addressing AI and machine learning (Petters, 2020). Additionally, AWS is, "pushing the boundaries of face, voice, and object recognition further." (Petters, 2020).

Where AWS truly lacks compared to its competitors is in its pricing structure. It is extremely hard to navigate their pricing structures making it hard to gauge a price range (Petters, 2020). Additionally, based on the pure size of the company it is very difficult to get individualized attention for companies (Petters, 2020). This could be a large deterrent for those companies that are new to the realm of cloud computing.

Table 6. AWS Strengths and Weaknesses

Strengths	**Weaknesses**
Experience	Pricing Structure
Computing Functions and Services	Reduced Professional Attention
Range of Options for Storage	Basic Backup Services
Depth of Tools and Technology	

2. Strengths and Weaknesses of Microsoft Azure

Table 7 provides a summary of the strengths and weaknesses of the main cloud computing offering from Microsoft, Microsoft Azure. In a similar nature to Amazon, Microsoft is able to pull on its experience as a tech giant to provide top of the line services to its customers with Azure. Through Azure, Microsoft has shown a commitment to the open-source communities. According to the Merriam-Webster Dictionary the definition of open-source software is, "having the source code freely available for possible modification and redistribution." (Open-Source, 2020). According to The Balance Careers, open-source software allows individuals to work on large projects to hone their skills while building a career in software development (Pickett, 2019). This shows a commitment to not only the large corporations but each individual.

Of the three providers listed, Microsoft Azure is the only provider to provide a hybrid solutions to their clients (Petters, 2020). This gives Azure an advantage in providing scalability and security to their clients. Additionally, the hybrid cloud gives a multitude of storage solutions allowing companies to store on private or public servers (Petters, 2020). On top of the hybrid cloud Azure also offers multiple backup services and website recovery functions that may be appealing to many potential clients (Petters, 2020). Lastly, given the compatibility of Microsoft programs and the availability of open source Azure allows scaling up and down at will with the added benefit of Microsoft investment in AI and machine learning (Petters, 2020).

While the pricing offered by Azure does provide flexibility to companies it is a little difficult to understand which results in the need to do some homework to know the best option (Petters, 2020). Lastly, since Microsoft is such a robust company there is the potential to not have great personalized service (Petters, 2020).

Table 7. Microsoft Azure Strengths and Weaknesses

Strengths	**Weaknesses**
Open-Source	Pricing Structure
Offers a Hybrid Cloud Model	Reduced Professional Attention
Offers More Than One Backup Service	

3. Google Cloud Platform

Table 8 provides a summary of the strengths and weaknesses of Google's cloud based system, Google Cloud Platform. Despite being a tech giant for many years now Google is well behind both AWS and Azure in terms of functionality. As shown in Chapter II, Google did not launch its first cloud service until 2013, 3 years behind Microsoft Azure and 11 years behind AWS. This lack of time on the market shows in their offerings.

What Google does well is allows for flexibility in their virtual machines supporting both Windows and Linux (Petters, 2020). Additionally, Google allows for you to utilize a pre-determined set-up or make a custom configuration for the platform (Petters, 2020). This flexibility is a shining point for many developers. Additionally, Google has the easiest to understand pricing structure. They essentially give their users a basic pricing structure for their basic services which are innovative in their own way but in their infancy (Petters, 2020).

Google's largest issue with their cloud service is their lack of storage solutions, mainly a lack of any backup options (Petters, 2020). This could be a major detractor to many consumers as one of the best advantages to the cloud is the storage abilities. Lastly, many of the tools and functions offered by Google are still works in progress which is clear

as they are still in their beta phases (Petters, 2020). This can be a disadvantage for many as there are large amounts of uncertainties when it comes to beta products. Most people like to know exactly what they are getting when they are paying for a service.

Table 8. Google Cloud Strengths and Weaknesses

Strengths	**Weaknesses**
Flexibility	Still Growing
Pricing	Storage Solutions
	Tools and Functions are a Work in Progress

E. COMING OF AGE IN THE DIGITAL AGE—ADVANCED STORAGE TECHNOLOGIES

System administration is a movement that abounds now. The themes involve automating everything, documenting everything and communicating as much as possible along with preserving and maintaining the level of security and privacy for government systems. Advanced storage technologies focus on network-accessible storage to combine network and mass storage technologies providing more flexibility for system administrators. Benefits include consolidation of storage and simplified administration. When coupled with cloud computing, researchers predict the United States will "see more change in the next decade than we've ever seen before in computer data storage (Harris, 2019, Paragraph 1)." "Twenty years ago, there were storage arrays—some small, some large —and tape for archiving. Now, the storage landscape is much more varied, ranging from PCIe SSDs with the performance of 2010's million-dollar storage arrays, to scale out storage capable of storing a hundred petabytes—a hundred million gigabytes—on low-cost commodity servers and automated enough that two people can manage the entire array." (Harris, 2019, Paragraph 3). With this growth of data, comes the necessity to develop new and innovative solutions to manage it and move, access and retain it as need be. Video via

consumer and for surveillance seems to be the main growth in the industry. The desire for greater granularity and specificity is also driving the markets. Twenty-five years ago, there were storage warehouses filled with government files and documents. At that time, "upgrades meant expensive new hardware and risky migrations, and the need to handle usage spikes meant the infrastructure was chronically over configured." (Harris, 2019, Paragraph 11). Now with the advent of cloud computing and gateways integrated in enterprise storage areas, it is difficult to discern what is going on—and even more challenging to determine if what is happening is cost effective.

Storage Global Server Farms—Have we really gotten away from large scale storage capabilities or merely replaced storage warehouse filled with paper and metal filing cabinets to warehouses filled with servers which make up cloud computing? A trend that is rapidly growing and has been in the last five years is the use of global server farms or cloud campuses. These are places where the cloud resides, where many commercial IT businesses "concentrate massive amounts of computing power in multiple data center facilities." (Miller, 2016, Paragraph 7). Now instead of warehouses, these fortresses are called data center hubs. "A server farm or server cluster is a collection of computer servers usually maintained by an organization to supply server functionality far beyond the capability of a single machine. Server farms consist of thousands of computers which require a large amount of power to run and to keep cool. To run at an optimum performance level, a server farm has enormous costs (both financial and environmental) associated with it." As an example, the biggest legal server farm is thought to be Google's and they are suspected to have over 1 million.

F. CONCLUSION

The essence of this chapter was to lay out the groundwork for where the government currently stands on its contract storage system and showcases their strengths and weaknesses. It concludes with a summary of what improvements can be made to present-day government contract storage system functionalities with emphasis on cloud computing as the wave of the future and what that entails for government contracting offices and personnel.

V. CONCLUSION

One thing that every contract administrator has heard at one point in their career is either, "document, document, document" or "if it isn't documented then it didn't happen." This just happens to be the life of anyone in the contracting career field. Many things can be said on the phone or out on the site but if that information has not been captured somewhere it is easily forgotten. Where the current systems lack is the interconnectibility to create a clear process of documentation for the most crucial contracting documents. Another issue is the ability to share the information between contracting offices at a moment's notice. This chapter provides recommendations and findings to improve the contracting process so issues like the above are solved in an automated or semi-automated manner.

A. FINDINGS AND RECOMMENDATION #1

1. Findings

The government is currently making vast strides to modernize their contracting systems to catch up to a quickly evolving technology industry. The Air Force and DoDEA have moved from antiquated systems such as physical paper storage and on-site servers to SharePoint and cloud-based systems with KT FileShare and CON-IT. With this migration to a cloud-based solution there are many considerations to be made.

The first consideration is whether government contracting should be considered for a cloud-based solution. The government has already started moving its contracting systems to a cloud-based solution with the implementation of KT FileShare as contract storage and CON-IT as the contract writing system. Both of these systems represent the government's belief that the near-future of government contracting is in the cloud. Looking at the groundwork laid out in the Cloud First Policy on what systems should be considered for migration to cloud-computing, contracting systems were ripe for that transition when CON-IT was implemented.

Contracting systems in general were reaching the end of their life cycles making new systems prime to be added to the cloud as the costs of migrating data would be reduced

overall. When instituting a new contracting system only those contracts that are currently on-going need to be migrated. Therefore, a vast majority of older contract or simple on time contracts would not have to make the migration to the new cloud-based service. This allows the government to focus more on the implementation of the new cloud opposed to worrying about the logistics and cost of migrating vast amounts of data to the new system.

Another question that should have been asked is, does the government need the ability to rapidly increase or decrease IT assets for a contracting system? With the natural ebbs and flows of the government workforce having the ability to increase or decrease assets without significant costs would be very beneficial. The ability to rapidly deploy additional assets would be extremely useful to a government contracting system especially at the end of the fiscal year. At this time of the year, contracting systems become taxed because there are significantly more concurrent users logging into systems at the same time. The ability to scale up resources for the months of, at a minimum, August and September would assist in getting the overall job completed.

Could a shift to a cloud-based system help the overall cyber security of contracting career field? Based on the information found in the NIST definition of a cloud computing system the security of information would more than likely be more secure but also more at risk. Since each contracting office would no longer have all of their own servers the resources that each base was using to secure their own servers would now be pooled in shared resources to protect one system of servers. On the other side of that the large pooling of resources would then make that site a "treasure pot" for a multitude of hackers or foreign enemies that wish harm to the United States.

Additionally, does it make sense for the government to control the cloud infrastructure itself or does it make sense to allow the program to sit in a cloud infrastructure at a commercial entity? This also ties into security as it helps determine who would be responsible for the security of data, a contracted company or the government. For maximum control, the government would prefer to maintain control of all facets of the cloud infrastructure. However, it also must be realized that the government itself is a large bureaucracy that does not move efficiently especially in the realm of IT. A properly written contract with a solid SLA could be very beneficial to the government. It would allow the

contractor to make upgrades as needed to both the infrastructure and technology staying current with the cutting-edge trends. This is something the government would struggle with since they would have to contract for each upgrade as it was released.

The most significant factor for moving to a cloud-based system is the reliability of not only the system but of the end users' network. This an area where the government needs to improve as more systems go to cloud based solutions. If the system is contracted then the contractor would be responsible for the server-side connection. A solid PWS and SLA would be needed to make the governments expectations clear to the contractor. In addition, this would address any remedies they government would have if the contractor were to miss the expectations of the government. These remedies would act as a way to motivate the contractor to maintain top class service to their government customer. The larger issue would be on the end user side. Government internet connections are buried behind firewalls and restrictions that make the connections spotty at best. Problems on the end-user's side would make a cloud-based system inaccessible. In order to continue the trend to a future in the cloud the government must make a concerted effort to ensure the internet connections provided to the end-users are extremely reliable.

Lastly, current technology must be considered as upgrades are completed. Based on the research conducted the cloud is the current state of the art system utilized in the commercial sector. However, as with all technology it will be quickly outdated. Many academic research efforts are focusing on the next best practice and all of them seem to deal with upgrading cloud computing. The government must be willing and able to adapt to a changing market as it seems upgrades like edge computing or multi clouds as well as open to new architectures like the software defining model. If the government fails to capitalize on emerging technology it will find itself in the same situation it was a few years ago, behind the times. Adapting is the only way the government will be able to compete with their near peers.

2. Recommendation

Continue with the current direction with contract generation and storage systems. Based on the findings of this thesis the government is headed in the right direction with

their contracting systems. The government is moving to a cloud-based solution to help maximize access from any location at any time. As these systems are further upgraded, it would be helpful to either have one system as a contract writing and storage system or to force the contract writing and storage systems to communicate. This would assist in all files integrating into a complete contract file. Additionally, as long as the government is moving to a cloud-based system there needs to be a clear focus on upgrading the existing IT infrastructure focused on reliable connections.

If the government considers contracting the cloud-based system out, then special care will need to be taken in the formation of that contract. The government will need to make sure that the Performance Work Statement (PWS) and SLA clearly address all roles and responsibilities of each party. In addition, the contractor will need to be consistently monitored for compliance to the contract. If compliance is not maintained the government must take swift action to remedy the situation with the contractor or replace the contractor.

B. FINDINGS AND RECOMMENDATION #2

1. Findings

Instantaneous or near instantaneous document sharing is something that does not happen in the government contracting realm unless you happen to be located in the same office and have access to the same servers. Something that would serve to expand the knowledge base of all contract personnel would be the ability to view documents that were created by many different contracting officers.

In order to do this all data would have to be stored in a central location or a shared system that every contracting personnel have access to do. The current system to positing contract opportunities is beta.sam. This system holds all government solicitations and documents that are attached. It is believed that all solicitations are held indefinitely in this system as there is no stated time that actions would be purged from the system. If this system could be expanded to include contract storage it could become the focal point of all federal contracts. Each person that is in a government contracting billet could be given access and allowed to search every file for key documents. This would expand the

knowledge of contracting personnel driving a better product and assist in the government getting a fair and reasonable price on all contracts.

If beta.sam is not an option then it would be recommended for the government to utilize some form of a hybrid cloud to serve this function. This could possibly be completed with the current systems in place as well. If KT FileShare is migrated to the cloud each contract office could be placed on their own private server while the generic contract information or the contract itself is loaded to a public server. A search could then be conducted on the public cloud by any contracting personnel for general requirements and a list could be generated of specific actions that may meet that criteria. The contracting personnel conducting the search could then be given links that provide one time read only access to files that match their search criteria. This would assist in the market research and cost/price analysis portions of contracts.

2. Recommendation

Based on our research, the authors of this thesis, recommend implementing a shared contract storage systems. One method could be by leveraging the new contract opportunities site (beta.Sam) as a potential storage resource for authorized users to review previous procurement actions or review it via a separate cloud storage platform. Another alternative would be to develop a site for all authorized government contract personnel to see data and store it using a hybrid cloud platform.

C. FINDINGS AND RECOMMENDATION #3

1. Findings

As stated in the recommendation the government has instituted two policies: the Cloud Smart and Cloud First policies. Neither of these policies gave the federal government's program offices clear direction on either how or when to migrate to cloud computing. When left to their own devices many program offices have seem to be risk adverse to the move to the cloud which is evident in the fact that the Cloud Smart Policy was created in 2011 but we are just now seeing the move to the cloud in contracting. It is obvious that the government needs clearer direction on cloud computing.

2. Recommendation

Another recommendation would be for the federal government to institute a special task force to study what really needs to happen with the cloud computing movement. Currently, and as this document revealed, all agencies are left up to their own devices for how to transition to a cloud platform provided they follow the policy guidance that was distributed to them. This has many agencies confused as to how to proceed and what the roles and responsibilities for IT personnel are in order to move this initiative forward. In a VAO article, dated 9/13/2018, 6 Enduring Problems in Federal Acquisition, the GAO highlights six problem areas agencies continue to face in contracting which have not been settled to date (these 6 were originally noted in 2007) (Virtual Acquisiton Office, 2018). Number 5 is cited as Federal procurement data: The government's main acquisition data repository, the Federal Procurement Data System-Next Generation (FPDS-NG), still contains unreliable data despite steps by GSA and the OMB to improve reliability (Virtual Acquisiton Office, 2018). GAO also cited limitations in FPDS-NG capabilities in the type of acquisition data it can monitor, as well as inaccurate data on OMB's IT Dashboard (Virtual Acquisiton Office, 2018). Back in 2018, cloud computing was not on the GAO's dashboard but we are sure if the writer updated the author, cloud computing would be added to the list (Virtual Acquisiton Office, 2018). Even though cloud spending is sky high at this time, there are no consistent rules and responsibilities that have been mandated to be followed. Accordingly, there is a necessity for a special task force to come up with a plan to address these inconsistencies and have agencies adopt some semblance of uniformity for cloud computing.

D. FINDINGS AND RECOMMENDATION #4

1. Findings

As stated earlier documentation is the key to a good contract file. Automating as many processes as possible reduces the risk that documents could be missed resulting is higher quality contract files.

2. Recommendation

At a minimum, the federal government should consider integrating and automating the data transfer between the multiple systems that are currently being utilized in the contracting career field. There should be automatic transfer of data between CON-IT, beta.sam, KT FileShare, and FPDS-NG. This should reduce the number of administrative mistakes that are caused by the manual moving of files through each system. Examples of this would be as follows:

Solicitations automatically post to beta.sam when released in CON-IT as all the applicable information is already entered in CON-IT. The solicitation documents would also automatically transfer to the applicable KT FileShare folders.

Awards automatically trigger the posting of an award notice based on the information input in the CON-IT award or FPDS-NG. Additionally, the signed award should automatically upload to KT FileShare upon release.

FPDS-NG data should automatically upload to KT FileShare the moment they are finalized.

This should apply to all amendments and modifications created on a contract.

E. POTENTIAL AREAS OF FUTURE RESEARCH

This thesis presents an introductory review of the current state of cloud computing and government contract systems. This thesis identifies potential areas that government contracting systems could utilize the cloud to exceed current expectations and standards. Further research into cutting edge technologies, specifically in document generation and storage should be further explored. Future research should specifically look at what is successful in the commercial marketplace and how it could be adapted to meet the government's needs.

Additionally, further research into the security implications of bringing cloud based document generation and storage will need to be completed. With more resources and systems being dedicated to the cloud in both the commercial and government markets, the

government will truly need to fully understand the security risks and mitigation strategy to fully utilize the potential of the cloud.

Lastly, further research into policy and procedures need to be reviewed. The most current policy was updated in 2018, which in the technology fields is a very long timeframe. Further research should be conducted in the cycles of applicable technologies to data generation and storage as well as the cloud. With this data recommendations can be made on the best times for the government to generate updated policies and procedures as it relates to acquiring cloud-based technologies. This would ensure that the government is not operating under outdated policy which in the long run hurts government readiness.

F. SUMMARY

Based on the discussion provided in this thesis, the federal government is quickly moving toward cloud computing as a data housing option for its procurements. However, security, reliability, and privacy aspects for data integrity still have to be clearly articulated to government contract personnel so that mishaps can be prevented. Unfortunately, as of this writing, adequate guidance has not been promulgated to the federal agencies in this regard.

Considering the recent VAO article, "Do Follow an Implementation Strategy, Don't Wing It," the recommendation is that agencies must follow a clear strategy to harness the full potential of cloud computing services, according to a recent report from the Securities and Exchange Commission (SEC) Office of Inspector General (OIG) (Virtual Acquisition Office, 2019c). The findings stated that although the SEC developed a strategy and goals for its cloud program, it instead used an "ad-hoc" or "as needed" approach to implement cloud computing (Virtual Acquisition Office, 2019c). The OIG determined that the SEC failed to: 1) Fully implement its cloud strategy; 2) Follow a clear strategic plan to evaluate and prioritize IT systems that needed to migrate to the cloud; and 3) Effectively track cloud-related goals (Virtual Acquisition Office, 2019c).

Further, the OIG cited that the agency did not coordinate or collaborate cloud strategies at an enterprise level (Virtual Acquisition Office, 2019c). Key stakeholders, such as the chief information officer and office of information technology officials did not work

together to review their agency's IT portfolio, the requirement and implement cloud computing best practices (Virtual Acquisition Office, 2019c). The OIG recommended that the agency reestablish a cloud computing governance committee that includes key stakeholders with authority to manage agency wide cloud-related acquisitions and systems' migration to the cloud (Virtual Acquisition Office, 2019c). The OIG also recommended the agency develop a roadmap and implementation plan for cloud migration that tracks related goals (Virtual Acquisition Office, 2019c).

Possibly this plan of action is what should happen in every federal agency now that the government is moving to cloud computing services. However, more astute, clear guidance has to be provided from the higher level governing agency so that proper strategy is followed and as was discussed previously an unbiased, independent task force should be enacted to study this movement in order to effect consistency across all federal agencies. Future recommended areas of study should include sound review of the Federal Government's Cloud Smart policy of 2019. The final version added emphasis on agencies to: 1) rationalize their application portfolios, which involves assessing the requirement for current applications and getting rid of old draining resources; 2) clarified language giving agencies discretion on acquisition of cloud technologies or develop their own; 3) Reestablish the role of the Federal Risk and Authorization Management Program (FedRAMP) in risk assessment and 4) adds workforce suggestions such as training employees on the use of new cloud technologies and reskill other workers. The Government's Cloud Smart policy is the blueprint and should be studied with focus on what is working and what needs to be tweaked or what isn't working and should be revamped. Much more emphasis should be placed on taking a deep dive for future investment in the cloud technologies to ascertain best practices across the entire federal government landscape.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Chief Information Officers Council. (n.d.). *From cloud first to cloud smart*. Retrieved May 17, 2019 from https://cloud.cio.gov/strategy/

ESDS. (2010, September 10). *Different types of data centers and their different tasks.* Retrieved July 31, 2018 from https://www.esds.co.in/blog/different-types-of-data-centers-and-their-different-tasks/#sthash.wSJGSGvI.dpbs

Figliola, P. M., & Fischer, E. A. (2015). *Overview and issues for implementation of the Federal Cloud Computing Initiative: Implications for federal information technology refrom management.* Congressional Research Service.

From cloud first to cloud smart. (n.d.). Retrieved June 3, 2021 from https://cloud.cio.gov/

Harris, R. (2019, May 28). *Data Storage: Everything you need to know about emerging technologies.* Retrieved from ZDNet: https://www.zdnet.com/article/innovations-in-data-storage-an-executive-guide-to-emerging-technologies-and-trends/

Kundra, V. (2011). *Federal cloud computing strategy.* The White House.

Mell, P., & Grance, T. (2011, September). *The NIST definition of cloud computing.* Gaithersburg, MD: National Institute of Standards and Technology.

Miller, R. (2016, May 18). *Scaling Up: Google building four-story data centers.* Retrieved May 31, 2021 from https://datacenterfrontier.com/google-building-four-story-data-centers/

Open-Source. (2020, May 22). Retrieved May 22, 2020 from https://www.merriam-webster.com/dictionary/open-source

Petters, J. (2020). *AWS vs Azure vs Google: Cloud services comparison*. Retrieved May 31, 2021 from https://www.varonis.com/blog/aws-vs-azure-vs-google/

Pickett, P. (2019, November 20). *How open-source software works.* Retrieved May 31, 2021 from https://www.thebalancecareers.com/what-is-open-source-software-2071941

Policies & priorities cloud smart. (n.d.). Retrieved June 3, 2021 from https://www.cio.gov/policies-and-priorities/cloud-smart/#:~:text=As%20of%20June%202019%2C%20the,safe%20and%20secure%20cloud%20infrastructure.

Sherman, B. J., & Freeman, E. (2007). Paperless Policy: Digital filing system benefits.

TechTarget. (2010, September). Data Centers: Owning vs outsourcing. *Enterprise CIO Descisions*, pp. 1-25.

Varghese, B., & Buyya, R. (2017). Next Generation Cloud Computing: New trends and research directions. *Future Generation Computer Systems*, 849-861.

Virtual Acquisition Office. (2019a). *Cloud spending and savings are up in the air.* Retrieved May 31, 2021 from https://www.gotovao.com/index.cfm?action=comment&v2&id=0300069545000443

Virtual Acquisition Office. (2019c). *Get cloud smart with OMB's final strategy.* Retrieved May 31, 2021 from https://www.gotovao.com/index.cfm?action=comment&v2&id=0300069901000443

Virtual Acquisiton Office. (2018). *6 enduring problems in federal acquisition.* Retrieved May 31, 2021 from https://www.gotovao.com/index.cfm?action=comment&v2&id=0300067644000443

Virtual Acquistion Office. (2016). *Basics of cloud computing.* Retrieved May 31, 2021 from https://www.gotovao.com/index.cfm?action=docs.file&id=0430060321000443

Virtual Acquistion Office. (2019b). *How Microsoft could win an $8B cloud contract without a bid.* Retrieved May 31, 2021 from https://www.gotovao.com/index.cfm?action=comment&v2&id=0300069224000443

Wang, S. (2019, November 15). Edge Computing: Applications, state-of-the-art and challenges. *Advances in Networks*, pp. 8-15.

Welchsman, L. (2015). *Managing chaos, digital governance by design.* Brooklyn: Rosenfeld Media, LLC.

Williams, H. (2018, March 13). *The history of cloud computing: A timeline of key moments from the 1960s to now.* Retrieved 11 October 2019 from https://www.computerworld.com/article/3412271/the-history-of-cloud-computing--a-timeline-of-key-moments-from-the-1960s-to-now.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California