A CLOUD GURU
A PLURALSIGHT COMPANY

Cloud and the Public Sector:

Challenges and Opportunities

Written by Chris Hughes
Managing Consultant - Cybersecurity at Oteemo | Cybersecurity Professor

FEBRUARY 2021

WHITE PAPER

Contents

INTRODUCTION

The Public Sector, and U.S. Government, has a long, often challenging history of cloud adoption. From the original "Cloud First" policy in 2011...

to the recently updated and released "Cloud Smart Strategy" in 2018, the Government has aimed to accelerate the realized value of cloud computing across the Federal Government.

However, public sector leaders have stressed the importance of cloud adoption within the Government and Department of Defense (DoD). Examples include former Federal Chief Information Officer (CIO), Suzette Kent, who discussed how **"leveraging cloud allows Federal agencies to better service their mission, drive improved citizen services and increase cybersecurity".** On the DoD side, you have statements from DoD CIO, Dana Deasy, who has stated that cloud is one of the four key components to digital modernization, and Gen. Shanahan, who as Director of the Joint Artificial Intelligence Center (JAIC), has stated that enterprise cloud is "existential" for A.I. across the DoD.

Despite that original policy being released nearly a decade ago, the Federal Government is still struggling to realize the full value of cloud computing. This is due to several challenges and unique requirements for IT consumption, cybersecurity and more as it relates to the Government and public sector.

Let's explore some of those challenges and opportunities.

CHALLENGE 1 SECURITY/COMPLIANCE

Rigorous security requirements often serve as the most significant impediment for cloud adoption within the public sector and Federal Government.

When it comes to challenges around cloud adoption, few are as cumbersome as security and compliance. This is particularly true in the U.S. public sector, where you have some of the most rigorous and time consuming compliance frameworks and requirements.

In addition to other relevant challenges related to the workforce, acquisitions, and more, the public sector grapples with a myriad of compliance requirements. Whether it is HIPAA, PCI DSS, NIST, FedRAMP or others, almost every organization is responsible for meeting requirements laid out in one or more compliance frameworks. Beyond the existing compliance frameworks, new frameworks and requirements continue to emerge, such as the Department of Defense (DoD)'s Cybersecurity Maturity Model Certification, which will require various security requirements depending on the data your organization is handling and a 3rd Party Assessment via a Third Party Assessment Organization (3PAO).

This often leads to a slew of security controls that must be met by the IT systems being implemented and put into production environments. These security requirements often cover various control families, such as Media Protection, Access Control, Personnel, and more. This equates to exponential man hours, dollars and time to both implement and document compliance with the controls that are applicable to the organization and system being developed or maintained.

Per Federal policy, cloud service offerings should be authorized for use prior to consumption by Federal agencies. That's where the Federal Risk and Authorization Management Program, or FedRAMP, comes into play. FedRAMP is a government-wide program that provides a "standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services" within the Federal Government. FedRAMP is tasked with assessing and authorizing cloud services for authorization and use across the Federal Government.

The issue is that this is a large ask, especially given the rapid proliferation of cloud services across the industry and the unique requirements and use-cases across various agencies. This creates a bottleneck for approvals with FedRAMP acting as a choke point. Going through the FedRAMP process is both expensive and time-consuming, creating a barrier for cloud providers who are reluctant (or can't afford to) commit the time and resources to get approval.

Couple these barriers with the rigorous security control baselines for offerings categorized at the High Impact level and it can be a challenge. In fact, of the 200+ approved FedRAMP approved cloud offerings, fewer than 20 are approved at the level of High Impact. Part of that is due to the fact that the High Level security control baseline contains over 400+ controls that a cloud service seeking authorization must meet.

Switching to the Department of Defense (DoD) side of the Federal Government, you have even more rigorous security requirements, which take FedRAMP baselines and add additional security controls, often referred to as "FedRAMP+". This means DoD leverages FedRAMP's assessment work but adds additional security controls due to DoD’s critical mission requirements. DoD authorizes cloud services based on the data associated with them, at various Impact Levels, ranging from 2,4, 5, and 6, with 6 being the classified environment.

Once services are authorized at their respective Impact Level, they receive what is referred to as a “DoD Provisional Authorization” or “P-ATO”, which means they are authorized for use within the DoD environment. All of these additional security controls mean even longer authorization timelines for the authorization and availability of cloud services within the DoD. This additional authorization overhead leads to a delay in access to innovative services and offerings for the DoD.

CHALLENGE 2 WORKFORCE

It’s no secret that organizations across all industries are struggling to attract and retain tech talent to facilitate their cloud migration and innovation goals.

Federal agencies such as the Labor Department often report large numbers of job vacancies, and cite issues such as the surging demand for technical skills. Industry organizations such as ISC2, who conduct annual workforce studies, report cybersecurity skill gaps that recently exceed numbers as high as 3 and 4 million.

This issue is more severe among public sector organizations, which have long struggled with attracting and retaining tech talent. This is for various reasons, such as long hiring timelines, strict location requirements, antiquated technology and lower pay and compensation than their private sector counterparts (to name just a few!). This issue is made even more severe due to the increasing number of Federal employees in technical categories are approaching retirement eligibility. This creates a desperate need for the Government to quickly and efficiently recruit and hire the best IT talent to fill existing vacancies, while also preparing future leaders to replace those approaching retirement.

WORKFORCE CHALLENGES IN THE PUBLIC SECTOR

Cybersecurity skill gaps

Long hiring timelines

Strict location requirements

Antiquated technology

Lower pay and compensation

CHALLENGE 3 ACQUISITION

State and Federal agencies, as well as the Department of Defense, are struggling with utilizing their existing acquisition models to acquire cloud services.

Cloud, unlike traditional IT consumption, utilizes metered services, which allow you to consume as much, or as little as is needed, scaling to meet demand, scaling down to realize cost savings and just simply providing a much more dynamic consumption model than is typical within IT. These consumption and rate-based pricing models are a massive change from traditional approaches to acquisition and don't fit well with the current methods available for departments and agencies across the Government.

Aside from challenges associated with acquisition and purchasing methods, the Government has also been mired by high-profile contract challenges, none of which are more known than the DoD's Joint Enterprise Defense Infrastructure (JEDI) cloud initiative, which aims to award a single CSP up to $10 Billion USD over 10 years as the unified cloud infrastructure across the DoD enterprise.

The DoD recently reaffirmed its award to Microsoft, but the initiative is being held up by protests from AWS, which ultimately means an enterprise cloud for the DoD is delayed. This is a big deal, especially given comments from the DoD CIO and senior DoD leaders on how critical enterprise cloud is for key capabilities such as AI and Machine Learning. It was reported that the DoD has spent over $5.3 Million administering the protested award already and over a year of legal battles. I would dive deeper into the JEDI saga of protests and delays, but that would require an entirely separate document of its own!

CHALLENGE 4 LEGACY SPENDING

Despite the Cloud First and Cloud Smart policies, on-premise IT infrastructure spending is not slowing down.

Despite the Cloud First and Cloud Smart policies, on-premise IT infrastructure spending is not slowing down. A recent report from the Office of Management and Budget (OMB) on IT Modernization notes that...

IT spending for on-premise infrastructure *actually rose* from 68% to 70% in recent years.

OPPORTUNITIES

Opportunities!? I know, I know, given all the challenges just laid out, it would seem that cloud adoption...

in the Public Sector and Federal Government is an impossibility, rife with too many challenges to overcome, right?

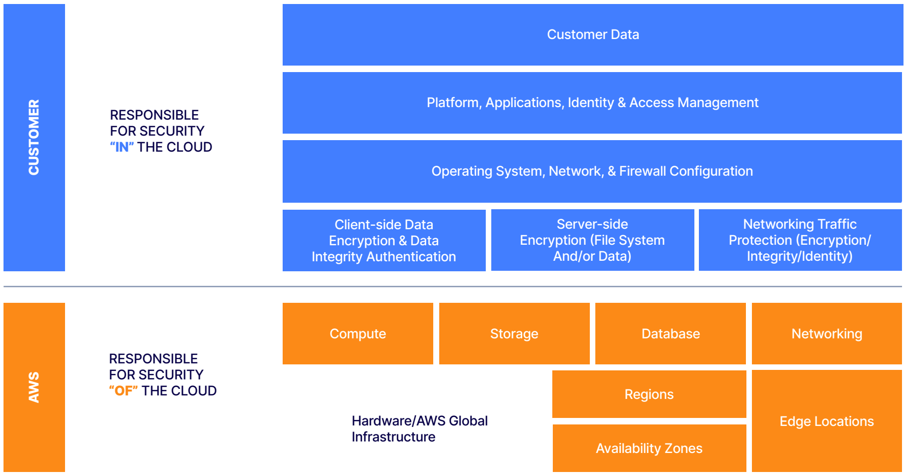
The reality is that, despite these challenges, the public sector is moving along its cloud journey. And, given its size, scope, requirements, and environment, it's a wholly unique journey. Let's look at some of the opportunities to help not only continue the cloud adoption journey within the public sector but potentially even expedite it.

OPPORTUNITY 1 SECURITY

Inheritance Models/Shared Responsibility Model

One of the primary benefits of cloud computing is the Shared Responsibility Model (which is often misunderstood, but that is a story for another day). The Shared Responsibility Model introduces a new paradigm where there is a partnership between both the Cloud Service Provider and the Cloud Consumer, or Customer.

Organizations are no longer responsible for the entire IT infrastructure, including physical hardware, equipment, facilities, and physical security. Customers can now consume cloud as a service, along with the accompanying reality that the Cloud Service Provider is responsible for much of the supporting underlying infrastructure and even operating systems and more, depending on the service model you're utilizing.


CUSTOMER
RESPONSIBLE FOR SECURITY "IN" THE CLOUD
Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network, & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System And/or Data)
Networking Traffic Protection (Encryption/ Integrity/Identity)
AWS
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
Compute
Storage
Database
Networking
Hardware/AWS Global Infrastructure
Regions
Availability Zones
Edge Locations

Using the AWS Shared Responsibility Model as an example, you can see that the CSP, AWS in this case, is responsible for security "of" the cloud. This means the underlying hardware, networking, facilities and more. And that is just in the Infrastructure-as-a-Service (IaaS) model. This share of responsibility increases if the Government makes use of managed Platform-as-a-Service (PaaS) and even Software-as-a-Service (SaaS) offerings, to include the CSP taking responsibility for operating systems, patches, upgrades and more. Given that the overwhelming majority of cloud data leaks occur on the customer side of the shared responsibility model, coupled with the stark workforce challenge for technical talent, it would behoove organizations to shift responsibility, where appropriate, to the CSP and focus on core competencies.

But what about security? Security isn't forgotten. Thankfully, as previously mentioned, there are programs and frameworks in place, such as FedRAMP and the DoD Security Requirements Guide (SRG), that help CSPs get their various Cloud Service Offerings (CSO)'s authorized at the level(s) that their Government customers are seeking, such as FedRAMP Moderate/High or DoD SRG Impact Levels 2/4/5 and 6.

These programs and frameworks provide Government customers a level of assurance that the services they're consuming have already been assessed by independent and neutral third parties and authorized (including Continuous Monitoring requirements) utilizing the same National Institute of Standards (NIST) 800-53 Security Control baselines the Government uses for their own IT systems.

However, it is incumbent upon the Government customers to leverage these existing authorizations and not try and re-assess what has already been done. Currently, this is not always the case. Many find FedRAMP and DoD SRG to be slow, impeding innovation and adoption, and preventing commercial parity.

CONTINUED... SECURITY

Inheritance Models/Shared Responsibility Model

Thankfully this is being addressed through various efforts. It was recently announced that FedRAMP is one step closer to being codified into law. If this occurs, the FedRAMP program will receive additional funding for resources and innovations to help expedite the authorization process, as well as more support for compliance among Federal agencies. FedRAMP is also working on innovative efforts to expedite the authorization process, such as the Open Security Controls Assessment Language (OSCAL) that they are pioneering along with NIST. This will help automate much of the traditional authorization process by making artifacts machine readable and integrated with assessment platforms.

This inheritance model is being leveraged not just for CSPs but also for platforms within the Government environments as well. The DoD, for example, has initiatives called Cloud One (C1D) and Platform One (P1). Cloud Onehas taken the approach of authorizing the underlying cloud infrastructure environment at the various DoD SRG Impact Levels (2,4,5, and 6) so that customers can inherit those security controls from the underlying cloud infrastructure. Platform One, an authorized DevSecOps environment built on top of Cloud One, provides multi-tenant environments where application owners within the DoD can use authorized environments, pipelines, and processes.

With Cloud One and Platform One, application owners don't have to repeat the process of building infrastructure and platforms, then getting them authorized for use. Instead, they can focus on capability/code delivery.
This ultimately equates to expedited capability delivery to warfighters and mission owners within the DoD.

OPPORTUNITY 2 COMPLIANCE

In addition to Federal and DoD specific security and compliance requirements, many public sector organizations have to wrestle with other compliance frameworks, such as PCI DSS, HIPAA, and HITRUST.

By leveraging cloud services which are already assessed against these compliance frameworks and authorized, public sector customers can rest assured they are using compliant services. This also helps them avoid the need to build and get these services/systems authorized themselves, so they can consume them as a customer while still meeting compliance requirements. Organizations can visit their CSP's compliance documentation to determine compliance with the frameworks of interest.

OPPORTUNITY 3 STATERAMP

Much like FedRAMP, which authorizes cloud services for the Federal marketplace, there is a new program...

called StateRAMP (stateramp.org) that provides States a standardized approach for protecting their data in the cloud. This provides a level of assurance to State Governments that the service offerings are secure and have been authorized with required frameworks and security controls. What is great about this program is that CSPs already authorized via FedRAMP will inherit the equivalent level of StateRAMP authorizations. This saves a tremendous amount of assessment/authorization time and money, helping expedite cloud innovation and adoption at the State level.

OPPORTUNITY 4 CONTINUOUS AUTHORITY TO OPERATE (cATO)

Another effort underway to expedite the traditional system assessment and authorization process is what is known as Continuous Authority to Operate (cATO).

The idea of On-Going Authorization/cATO is certainly not a new concept, and has been part of the Risk Management Framework (RMF) dialogue since its inception, but it has long proven elusive for most organizations/agencies and often just a buzzword.

However, agencies such as the General Services Administration (GSA) and FedRAMP are working to operationalize the concept and make it a reality.

This innovation is also taking place within the DoD, particularly with the U.S. Air Force (USAF) where you have programs such as Kessel Run and Platform One. Platform One is the first DoD CIO approved DevSecOps Service Provider within DoD, and is helping lead the way towards making cATO a reality. The cATO process will include a three-pronged approach of authorizing the platform, process and teams so that software promoted through the systems/pipelines will not need

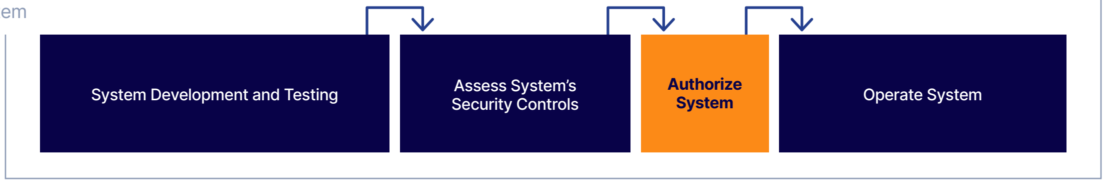
CONTINUED... CONTINUOUS AUTHORITY TO OPERATE (cATO)

to be reauthorized every time a software release or promotion occurs. By authorizing the platform, process and team(s) and utilizing CI/CD control gates of pass/fail, cATO allows teams to continuously deliver code and capabilities to the warfighter, without the often arduous ATO cycle that is commonly repeated every few years.

Below is a good depiction of the traditional authorization process, compared to the planned cATO process, which will be accompanied by an upcoming cATO Guidance document to the DoD in early 2021.

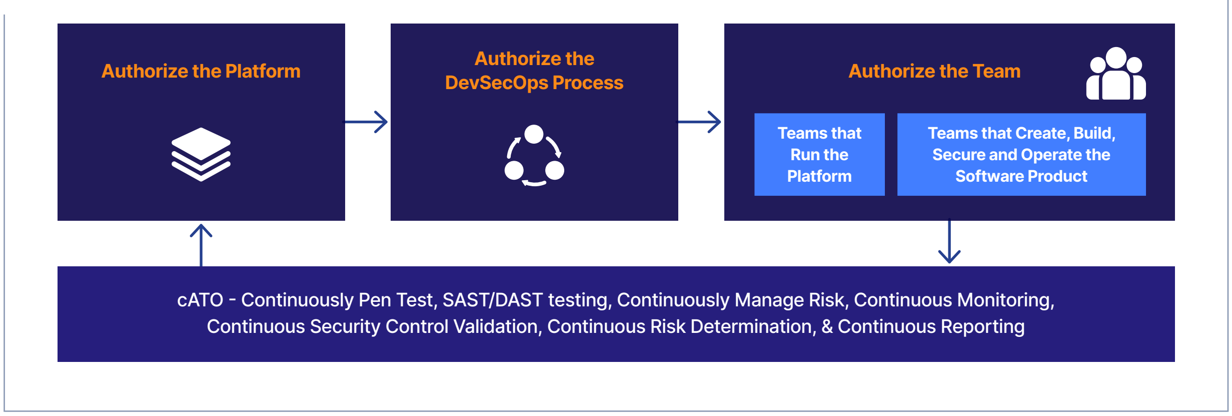
Traditional Authorization Approach

Authorize System


System Development and Testing
Assess System's Security Controls
Authorize System
Operate System

Continuous Authorization Approach

Authorize Platform, Process, Team


Authorize the Platform
Authorize the DevSecOps Process
Authorize the Team
Teams that Run the Platform
Teams that Create, Build, Secure and Operate the Software Product
cATO - Continuously Pen Test, SAST/DAST testing, Continuously Manage Risk, Continuous Monitoring, Continuous Security Control Validation, Continuous Risk Determination, & Continuous Reporting

OPPORTUNITY 5 LOW IMPACT SOFTWARE AS A SERVICE (LI-SAAS)

Agencies such as GSA are also pioneering innovative authorization processes.

Li-SaaS addresses the quickly proliferating SaaS utilization across GSA (and the Government), allowing for a more flexible authorization process that is less cost-prohibitive and provides a streamlined assessment for application SaaS offerings working with low impact data. Other public sector organizations and agencies can model this approach to allow access to innovative SaaS offerings for their organization, while still considering fundamental security concerns.

OPPORTUNITY 6 WORKFORCE

Remote Work

Many Government agencies and departments have supported remote work but on a limited basis for years. However, with the COVID situation, the Government has experienced a massive surge in the remote workforce. Several agencies have even experienced increased productivity with the increase in remote work and many speculate that many Government and public sector employees may stay working remotely permanently.

This surge was largely facilitated due to, you guessed it, cloud computing. Whether it is email, document collaboration, video calls, or other cloud service offerings, the cloud's robust infrastructure was perfectly positioned to support a suddenly distributed workforce.

This isn't lost on senior leadership and many have praised the role that cloud has played. This has also led to increased cloud adoption among public sector customers and has helped expedite many organizations' digital innovation/transformation efforts.

Recent comments from the DoD Deputy CIO, John Sherman, support this reality, where he mentioned that **over a million users are making use of their Commercial Virtual Remote (CVR) environment since March of 2020.** Mr. Sherman praised this accomplishment as nothing short of amazing and something that should serve as the gold standard for Government.

With this remote workforce paradigm here to stay, we will see increased cloud adoption and reliance by the public sector, and with it, increased innovation and service offerings from CSPs catering to public sector customers.

CONTINUED... WORKFORCE

Remote Work

This remote work paradigm and realization of its effectiveness also provides a pathway for the Government to change its hiring and workforce requirements. Rather than requiring positions to be specifically located somewhere, instead, **many IT related roles can be located anywhere across the country. This opens up the talent pool massively, and also presents potential cost savings, as cost of living adjustments are accounted for in salaries.**

It also creates a more resilient workforce that isn't geographically confined and susceptible to location-specific incidents (sound familiar to Incident Response/Business Continuity of cloud architecture?)

This remote work is facilitated by cloud computing and cloud will continue to play a pivotal role in this new work paradigm for most organizations, including the public sector.

Training

Remember that workforce challenges I mentioned? The skills gap, and the additional challenges on top of that faced by public sector organizations? Those challenges are real, and are only going to be exacerbated by the surge in cloud adoption and consumption in the public sector. Thankfully, there is no shortage of affordable and excellent training options for public sector customers to upskill their existing workforce.

A Cloud Guru is a perfect example. I first stumbled upon ACG several years ago, around the same time I got exposed to cloud. I knew nothing about cloud but ACG helped fix that issue. I was able to utilize ACG courses, among other learning resources, to pass 8 AWS certifications along with some Azure. Whether it was blogs, video courses, or built-in lab environments, I was able to use these tools to learn the platforms and environments, as well as the security capabilities of the cloud platforms that my Government employers/customers were leveraging.

This in turn helped me advocate for cloud adoption and the security innovations that the cloud offers.

Being able to spin up on the spot learning environments where I could practice with services and configurations was invaluable. The best part was that it was affordable and I could take it with me on the go, via the ACG mobile app, if I was traveling, working out, or just lounging around the house.

This is an excellent method for public sector organizations to purchase subscriptions and allow their workforce to learn and train with the platforms and technologies they're adopting, increasing cloud fluency across their organizations and also minimizing security risks by preventing situations such as misconfigurations. A trained workforce is a capable workforce.

CONTINUED... WORKFORCE

Mission Impact

While the public sector still has a ways to go and will likely always struggle to compete with private industry in terms of compensation, one thing they do offer that the private sector often can't is Mission Impact.

Whether at the State and Local level, or at the Federal level with agencies providing citizen services to millions of citizens, the potential for impact is huge. This also applies to DoD organizations such as the U.S. Army's newly formed Enterprise Cloud Management Office (ECMO), the U.S. Navy's DevSecOps effort, dubbed "Black Pearl", or the previously mentioned U.S. Air Force Platform One initiative. Through all of these, the ability to leverage cloud while assisting national defense is unparalleled.

These are opportunities that the private sector often cannot compete with in terms of impact and sense of purpose. Public sector organizations should leverage this message in their pursuit of tech talent and demonstrate that you can work with innovative cloud technologies while working in the public sector.

Acquisition

DOD CLOUD ACQUISITION GUIDEBOOK

Defense Acquisition University (DAU) recently released the DoD Cloud Acquisition Guidebook in response to the reality that many organizations are struggling with how to use current acquisition models to obtain cloud services. This guidance helps programs determine how to take advantage of the opportunities provided by cloud services and what contracting models help facilitate that.

ADAPTIVE ACQUISITION FRAMEWORKS

Public sector organizations, such as the DoD through the Undersecretary for Defense, Ellen Lord, are implementing "Adaptive Acquisition Frameworks" with the goal of speeding up DoD acquisition and leading to greater innovation and purchasing of advanced technologies, including cloud. Other public sector organizations are likely to follow suit and implement new acquisition and contracting models to try and alleviate the struggles associated with purchasing cloud services.

CIA C2E AWARD

Despite challenges within DoD around cloud contract awards, the Central Intelligence Agency (CIA) has pushed on, recently announcing its long-awaited Commercial Cloud Enterprise (C2E) contract. This was awarded to multiple CSPs, which included AWS, Microsoft, Google, Oracle and IBM. This award makes multi-cloud in a large public sector agency a reality and at the biggest scale yet, given the award is expected to be worth several billion dollars. This shows that large cloud acquisitions CAN be done within the public sector and that cloud is viable even for some of the most secure and sensitive workloads.

CONTINUED... WORKFORCE

Acquisition

EVENTUAL JEDI AWARD

Despite its long and challenging history, the JEDI award for the DoD seems to be still on track to eventually become a reality. The DoD CIO recently reaffirmed the DoD's commitment to the award and stressed the importance of an enterprise-wide cloud capability for the DoD and how pivotal it is for dependent efforts around AI and Machine Learning. Whether through JEDI or another method, the DoD will implement an enterprise-wide cloud environment that will support the U.S. National Defense and be utilized by millions of soldiers and civilians across the DoD. It is also worth noting that one key requirement/goal of JEDI is "commercial parity" with public commercial cloud service offerings. This will help mitigate the constant lag time of access to commercial innovation that the DoD experiences with cloud.

Legacy Spending

Remember how I mentioned much of the Government's IT budget still goes to legacy spending? While that isn't likely to change overnight, it will show an increased shift towards modernization. Through the surge in the remote workforce and the reality that cloud computing offers the government flexible and resilient services and capabilities, public sector organizations will increasingly invest their resources into cloud.

SUMMARY

While there is no shortage of challenges of cloud adoption in the public sector, it is clear that there is also tremendous room for opportunities.

Public sector organizations are increasingly becoming reliant on cloud services to maintain resilient services and capabilities for their respective missions and purposes.

Through the work of innovative process overhauls and strategic leadership, some of the trailblazing efforts mentioned above will have spiraling impacts across other Federal, State, and Local organizations/agencies as they continue on their own respective cloud journeys.

It is paramount that organizations don’t forget the most critical piece of the puzzle along that journey, the workforce. It is key that organizations invest in their people, provide learning paths, incentives, and room for growth. Whether it is upskilling existing staff, hiring new resources with key competencies, or partnering with trusted consultants and advisors who have proven themself in this space, the workforce will be the most critical component of cloud adoption success in the public sector.

Your organization’s cloud journey success depends on it.

Chris Hughes

Managing Consultant - Cybersecurity at Oteemo | Cybersecurity Professor

Chris has nearly 15 years of IT/Cybersecurity experience. This ranges from active duty time with the U.S. Air Force, a Civil Servant with the U.S. Navy and General Services Administration (GSA) as well as time as a consultant in the private sector. In addition, he also is an Adjunct Professor for M.S. Cybersecurity programs at Capitol Technology University and University of Maryland Global Campus. Chris also participates in industry Working Groups such as the Cloud Security Alliances Incident Response Working Group. Chris holds various industry certifications such as the CISSP/CCSP from ISC2 as well as over 8 certifications from leading Cloud Service Providers such as AWS. He regularly consults with IT and Cybersecurity leaders from various industries to assist their organizations with their Cloud migration journeys while keeping Security a core component of that transformation. Chris currently works at Oteemo, where he serves as a Cloud Security SME for the U.S. Air Force Platform One initiative, as well as consulting with other Public and Private sector organizations on Cloud-native security best-practices, along with the rest of his Oteemo team who specialize in cloud and digital transformation acceleration.

About A Cloud Guru

The leading platform for cloud learning

A Cloud Guru (ACG) is driven by a simple mission: to teach the world to cloud. We believe people learn best by doing. That’s why our in-house cloud experts go to ridiculous lengths to design fresh, engaging, and hands-on learning tools that empower both individuals and organizations to stay ahead of the technology curve. As the world’s most comprehensive, hands-on, and effective platform for cloud learning, ACG has enabled more than 2 million learners and 4,000 organizations to achieve a brighter future.