

Security Considerations for DoD Cloud Migrations

White Paper

2 October 2017

Buchanan & Edwards, Inc.
1700 North Moore Street
Suite 2110
Arlington, VA 22209

Frank Hellwig
Director of Engineering

1. Introduction

This white paper discusses security considerations for U.S. Department of Defense (DoD) cloud migrations. Unlike commercial or U.S. Government cloud migrations, DoD cloud migrations are additionally governed by regulations from the Defense Information Systems Agency (DISA) and other DoD organizations. This paper covers security-related topics related to migrating DoD systems into commercial or government-specific cloud environments.

The target audience is executives, program managers, and technologists (in both contracting and the Government) that work with Information Systems Security Officers, accreditation authorities, and cloud service providers involved with DoD system cloud migration efforts and require familiarity with the security requirements surrounding these types of cloud migrations.

1.1 Document Overview

For this paper, we assume that the systems under consideration must meet the security controls associated with DISA information impact levels 4 or 5. Impact level 2 is intended for open (public) data while impact level 6 is reserved for classified systems that are beyond the scope of this white paper.

From a conceptual point of view, we focus on typical Line of Business (LOB) applications that process Controlled Unclassified Information (CUI) in on-premises data centers or in ad hoc server environments. The regulations under discussion are agnostic to the origin platform and only concern themselves with the sensitivity of the data being processed. We state the conceptual point of view here to orient the reader in envisioning a typical cloud migration scenario.

Our experience has shown that security considerations are often the most protracted component of any cloud migration effort and planning accordingly is critical to such migration efforts. In this document, we highlight key security topics and their relevance to migrating DoD enterprise system into the cloud.

1.2 Document Organization

This document is organized into four main sections. First, we present a typical DoD LOB system architecture. Second, we discuss the security implications of a future-state cloud architecture. This includes requirements, policy, and risk mitigation strategies. Third, we provide a conclusion and summary. Fourth, and finally, we offer a reference list of security resources that are both normative and informational in scope.

1.3 Caveat of Coverage

There is a substantial amount of documentation, policies, procedures, standards, regulations, orders, and guides that apply to cloud systems and ongoing cloud operations. This white paper is a high-level view of selected topics. The intent is to highlight specific areas and draw attention to elements that require planning and an elevated awareness as DoD organization migrate CUI system into the cloud.

2. Architecture

Figure 1 shows a conceptual DoD LOB application consisting of various components hosted within a data center. The network connectivity both between the system components and the end users is via an internal network. The cloud migration effort shown in the figure illustrates how these components can be allocated to various cloud service models. The cloud service models are discussed in section 3.5.

Of specific note is the necessity for a secure network (i.e., NIPRNet) as the means of connecting users to the cloud via a gateway called the Cloud Access Point (CAP). Not shown in this diagram are infrastructure details such as user directory services or ancillary services such as auditing and cloud management.

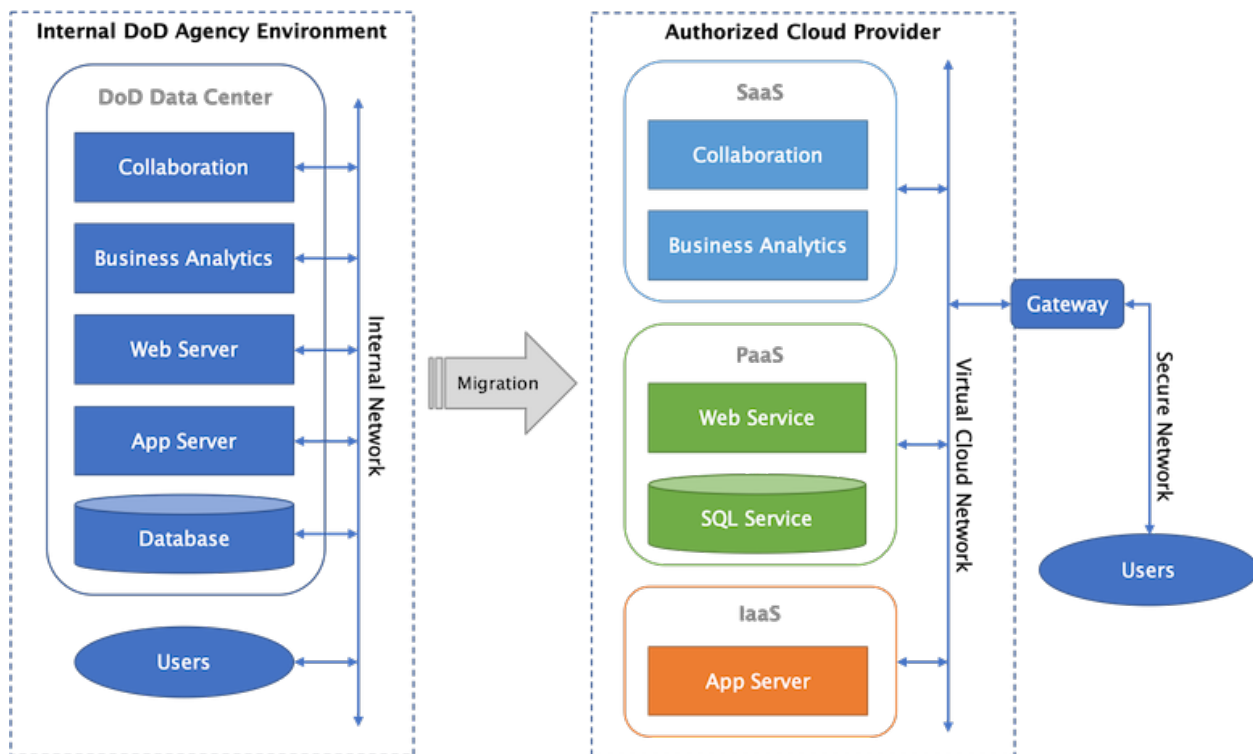


Figure 1 - Migrating a typical LOB application means selecting the appropriate cloud models, achieving the required network connectivity for user access, and securing the authority to operate the system.

Within the context of this dynamic architecture are many complicated facets that are technical, procedural, and regulatory. The aspect of security is one that involves all three of those facets.

The remainder of this document addresses the security considerations for migrating this type of system into a cloud environment. This is a non-exhaustive set of topics including FedRAMP controls; shared information assurance responsibility; user access and security; technical security guides; cloud service models; and cloud service offerings authorized by the FedRAMP process.

3. Security Considerations

This section presents a set of topics that reference normative regulations and provide points of further discussion for the DoD cloud migrations. Each subsection concludes with a paragraph offering brief recommendations on the topic.

3.1 Government Security Controls

In 2011, the U.S. Government issued a Cloud First policy requiring that federal agencies migrate selected services to the cloud in accordance with specific mandates. These same agencies had existing security requirements for their information systems as required by the

Federal Information Security Management Act (FISMA). This act is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law as part of the Electronic Government Act of 2002.

Rather than having each agency conduct the work ensuring that their cloud infrastructure meets the specific impact controls mandated by FISMA, the U.S. Government created the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP streamlines processes and reduces costs by conducting independent security assessments of CSPs. As part of the Cloud First policy, agencies must procure cloud services from a FedRAMP-authorized CSP.

3.1.1 FISMA and FedRAMP Controls

Both FISMA and FedRAMP compliance is achieved by meeting the controls identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems.” There are three levels (low, moderate, and high) in the FISMA and FedRAMP baselines. Table 1 shows the number of controls for each level. Note that there are additional FedRAMP controls that are specific to cloud environments.

Table 1 - NIST SP 800-53 controls for FISMA and FedRAMP baseline levels.

	Low	Moderate	High
FISMA	124	261	343
FedRAMP	125	326	421

3.1.2 DISA Impact Levels, the Security Requirements Guide, and FedRAMP Plus

Whereas FISMA and FedRAMP apply to the entire U.S. Government, DISA has specified its own information impact levels and has provided a Cloud Computing Security Requirements Guide (CCSRG) that builds on the FedRAMP requirements. The CCSRГ also defines additional security controls that are given the FedRAMP Plus (FedRAMP+) label.

The DISA impact levels are defined by a combination of the sensitivity or confidentiality level of the information and the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information. There are currently four impact levels (level 1 was removed and merged with level 2 while level 3 was removed and merged with level 4). The DISA impact levels are now 2, 4, 5, and 6.

The DoD Cloud Computing Security Requirements Guide (CCSRG) identifies the requirements

associated with the information impact levels. Broadly speaking, FedRAMP moderate is required for level 2 while FedRAMP moderate (supplemented with DoD FedRAMP+ controls) or FedRAMP high is required for levels 4 and 5. DISA impact level 6 is for classified information and is not further discussed in this white paper.

For impact level 4 or 5 information, the CCSRG requires a FedRAMP moderate or high baseline including additional security controls specified by the FedRAMP+ requirements. The CCSRG defines FedRAMP+ as the concept of leveraging the work done as part of the FedRAMP assessment and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements.

For a FedRAMP moderate baseline, FedRAMP+ imposes 38 additional controls for impact level 4 information and 48 additional controls for impact level 5 information. For a FedRAMP high baseline, FedRAMP+ imposes no additional controls for impact level 4 information and only 10 additional controls for impact level 5 information.

3.1.3 Authority to Operate

Unless an agency directly sponsors a CSP for an Agency Authority to Operate (ATO), deploying a system to a CSP involves two steps. The first step is selecting a CSP that has received a Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO). The JAB is comprised of officials from the General Services Administration (GSA), Department of Homeland Security (DHS), and the Department of Defense (DoD). It is provisional because each agency itself must have its own ATO before it can use the specified services offered by the CSP. Achieving the agency ATO is the second step and leverages the work accomplished by the P-ATO assessment.

3.1.4 Recommendations (Government Security Controls)

For many DoD systems, an environment suitable for processing information at impact level 4 or 5 will be required, supplemented with the appropriate FedRAMP+ controls. This means that a FedRAMP moderate or high baseline is required with the additional FedRAMP+ controls specified in the CCSRG. BE recommends that RFP authors consider the guidelines in the DoD CCSRG and specify, without ambiguity, the FedRAMP baseline and any additional security control that may be required by the baseline. The Cloud Security Information Impact Level Matrix referenced in section 5.1 can be used to determine the impact level.

3.2 Shared Responsibility

There is, occasionally, a misconception that selecting a cloud service provider and their FedRAMP-baselined cloud service offering is sufficient for deploying an operational system into the cloud. Terminology such as the Provisional Authority to Operate (P-ATO) further confuses the issue by giving the impression that there is an ATO in place for that cloud service provider. Nothing could be further from the truth. A P-ATO simply means that the CSP has been verified, by a third party, as following a selected set of security controls. It does not give an agency, department, or organization the authority to deploy and operate a DoD application in the cloud or connect users to such an application.

As a case in point, let us consider the guidance from the Department of the Navy. In April 2016, the Navy's office of the Chief Information Officer presented a briefing titled "DON Cloud Update." This comprehensive briefing addressed topics including policy, current efforts, cloud governance, management models, and the certification process. There are two important points in the briefing that are significant enough to be reiterated in this white paper.

The first point is the division of Information Assurance (IA) requirements between the CSP, the Navy, and the system owner. Figure 2 is copied directly from the Navy's Cloud Update briefing. It illustrates that, while the security controls for part of the infrastructure can be inherited, the system owner must secure their own per-application authorizations. Simply procuring an agency ATO for a CSP is not sufficient. The internal IA requirements must be met before a system becomes operational in the cloud.

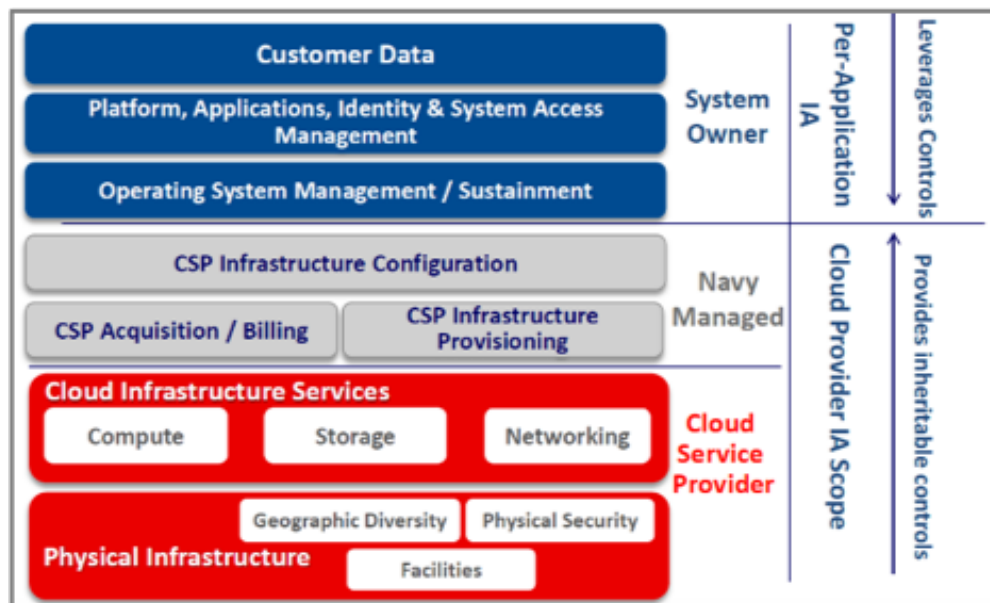


Figure 2 - System, Navy, and CSP IA security responsibilities.

The second point is that, regardless of any CSP ATO, all "Navy information systems are still required to meet all DoD instructions (e.g., 8500), Joint Chiefs instructions (e.g., 6510), and USCC CTOs (e.g., 07-12/HBSS)." The critical message is that migrating to the cloud does not eliminate any existing policy requirements.

3.2.1 Recommendations (Shared Responsibility)

BE recommends that these two points be taken together and that overlap between system and inherited controls be mapped against current policy requirements so that overlap is identified (reducing time and cost) while also ensuring that no gaps exist between the controls satisfied by the CSP's ATO and applicable agency and DoD policies.

3.3 User Access, Authentication, and Authorization

Deploying a system from an internal environment to the cloud changes how users access the application and, potentially, how they are authenticated and authorized. Migrating a DoD system into the cloud changes the access route for users because a cloud endpoint (outside the internal network) must be accessed via NIPRNet as shown in Figure 3.

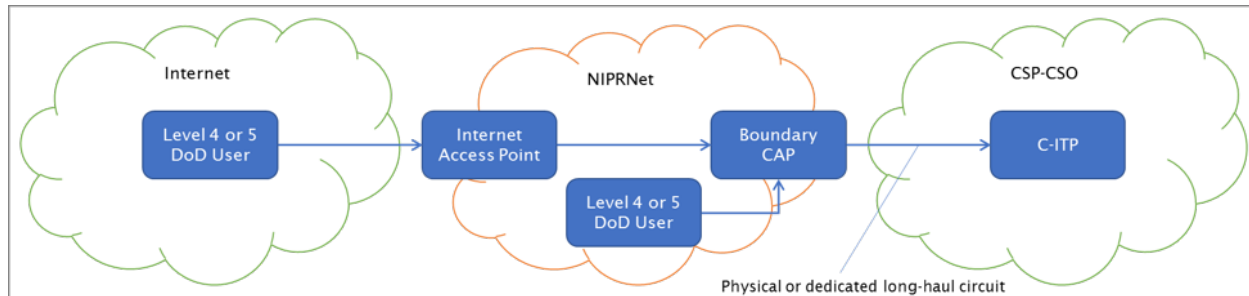


Figure 3 - Connecting to the cloud for DoD users involves several networks and endpoints.

Connecting to a DoD system in the cloud involves one or possibly two components. Users within DISN's NIPRNet can access the Cloud Information Technology Project (the C-ITP – i.e., the DoD application or system) via a Boundary Cloud Access Point (BCAP). Users not within the DISN (i.e., external internet access) must go through an Internet Access Point (IAP) and from there transition through the BCAP to the C-ITP.

3.3.1 Access Points

The CCSRG mandates that all controlled unclassified information be accessed via a CAP. The CAP establishes a boundary between the defense network and the CSP's service offerings. It provides the capability to detect and prevent cyberattacks from reaching the DoD Information Network (DODIN). Depending on the CSP, provisioning connectivity through a CAP can incur substantial time. Therefore, the organizations should begin the analysis of NIPRNet connectivity early in the process.

The IAP is essentially a virtual private network within the NIPRNet demilitarized zone connecting an external user to the CAP. The IAP protects NIPRNet from external threats. The DoD Cloud Connection Process Guide (CCPG) gives further, in-depth guidance on the IAP connection requirements and the processes for establishing connectivity to external users.

3.3.2 Public Key Infrastructure

According to section 5.4 of the CCSRG, CSPs are required to provide DoD Public Key Infrastructure verification for user verification. This typically means some type of Personal Identity Verification (PIV) token – for the DoD, this would be the Common Access Card (CAC). What is interesting about section 5.4 is that it refers to accessing the CSP configuration itself (i.e., the configuration portal for Azure or AWS). It further caveats this by stating "Whenever a CSP is responsible for authentication of entities and/or identifying a hosted DoD information system, the CSP will use DoD PKI certificates in compliance with DoDI 8520.03."

This must be considered when analyzing the security requirement of a DoD system deployed

to the cloud. Strictly speaking, the system (or system owner), not the CSP, is responsible for the authentication of entities. The application itself must provide the infrastructure to authenticate users via their CAC. The system must be populated with (or have access to) the public certificates of all authorized users. Also, it must have access to the Certificate Revocation List and updates this list in accordance with established procedures. Once identified, the DoD ID (EDIPI) from the CAC can be used to perform authorization decisions regarding the various application and administrative components of the cloud system.

3.3.3 Beyond the CAC

Over the past few years, there have been discussions for replacing the CAC with an alternate identity verification system that may be based on behavior patterns and biometrics. While still in the future, the multi-year plan for some DoD cloud migrations could intersect this timeline. System engineers and architects should become aware of these initiatives and plan accordingly.

3.3.4 Joint Regional Security Stack

The Joint Regional Security Stack (JRSS) is a new DISA initiative that collocates and combines the current ad hoc landscape of security devices into a single, performant equipment suite. Physically, it consists of up to 20 equipment racks that perform firewall functions; intrusion detection and prevention, virtual routing, and many other network security capabilities. The CCPG notes that IAPs and CAPs may integrate with a JRSS providing additional layers of security to defend against threats from using the CSP.

3.3.5 Recommendations (User Access, Authentication, and Authorization)

BE recommends that the network topology be determined early in the process and that connectivity through the JRSS and the CAP be analyzed so that bandwidth requirements can be met and that the current and expected user base will have reliable connectivity. Furthermore, we recommend that the identity management framework be structured such that it is consistent with cloud identity management models and that both current (i.e., CAC-based) as well as future verification mechanisms be considered in the planning phases of migration efforts.

3.4 Security Technical Implementation Guides

While Security Requirements Guides (such as the CCSRG) are broad in scope, covering an overall technology or product family, Security Technical Implementation Guides (STIGs) focus on a specific technology area (such as application development) or even a specific product (such as the Oracle database).

3.4.1 Anticipating Technologies and Products

Existing DoD systems have complied with a specific subset of STIGs. When such a system is reengineered for a cloud environment, the system will require revalidation against many of these same STIGs. In addition, STIGs that were previously inapplicable will now be mandated

with a cloud system. For example, there are five STIGs that apply to various Linux versions. If the target environment is Linux, then these will come into play.

3.4.2 Recommendations (Security Technical Implementation Guides)

Working through a STIG often requires collaboration between the Information System Security Officer (ISSO) and the engineering team. The engineering team reviews the rules and, based on their first-hand knowledge of the system, assesses each rule as open, not a finding, or not applicable. BE recommends that the appropriate STIGs be identified early in the process – especially with respect to new technologies not currently in use.

3.5 Cloud Service Models

In this subsection, we will review the three broad service models currently offered by CSPs. This is not itself a security topic but identifying these defines a common language that is relevant when looking at FedRAMP authorizations.

When a FedRAMP authorization has been granted, it is often scoped to one or more of these service models offered by a CSP. Within those models, there may be finer grained levels of restriction that specify individual services within each service category. Understanding these, therefore, has implications for both security and overall cost.

Cloud service providers offer varying levels of operational support. They vary in the type and number of resources managed by the customer versus those managed by the service provider.

Table 2 compares the resources supported by the customer, agency, or organization against those managed by the service provider for each service model. On the left is the non-cloud (on premises) solution where the customer manages all physical and computing resources. From there the number of resources supported by the cloud service provider increases from the left to the right.

Table 2 - Cloud service models provide varying degrees of agency and CSP support responsibilities.

On-Premises	Infrastructure-as-a-Service (IaaS)	Platform-as-a-Service (PaaS)	Software-as-a-Service (SaaS)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime

Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Legend (color key):			
Supported by the Customer/Agency/Organization		Supported by the Cloud Service Provider	

3.5.1 Cloud Migration Case Studies

The author of this white paper co-chairs the American Council for Technology-Industry Advisory Council (ACT-IAC) Cloud Migration Working Group and, in that capacity, has collated many cloud migration case studies by various government agencies.

Reviewing these case studies has revealed that most cloud migrations are either of the Infrastructure as a Service (IaaS) or the Software as a Service (SaaS) variety. The IaaS service category represents the typical “lift and shift” scenario when virtualizing a data center. The SaaS service category is typified by the move to an Office 365 environment.

The Platform as a Service (PaaS) model is the middle ground where, for example, instead of purchasing licenses for and installing SQL Server and IIS, the customer takes advantage of these being offered as services. Internally, the CSP may still run the original software on a platform of their choosing, but the service user is freed from managing the application or configuring the underlying operating system.

From BE’s own work in cloud migration, PaaS usually results in lower cost for commodity software over the IaaS model, both in terms of up-front acquisition and installation costs as well as operational administrative and licensing costs.

3.5.2 Recommendations (Cloud Service Models)

Moving from the data center to the cloud can be as simple as creating a one-to-one mapping from local servers (physical or virtual) to corresponding instances in the cloud. But doing so does not recognize the value that Platform and Software as a Service can offer. Adopting these, when possible, can result in substantial cost savings as well as an enhanced security profile.

If the CSP has already been authorized to provide specific services as part of a FedRAMP baseline, then leveraging these reduces the cost for accreditation, STIG compliance, and operational security maintenance and upgrades. BE recommends that the organizations examine which components of their system can leverage a higher-managed service model.

BE also recommends that the DoD organizations develop an up-front strategy and a set of standards for leveraging security controls in specific service models and platforms (e.g., AWS or Azure) to maintain consistency, repeatability and compliance.

3.6 Cloud Service Offerings

The individual services provided by a CSP are called the cloud service offerings. In a broad sense, these are the IaaS, PaaS, and SaaS service models discussed in the previous section. On a narrower level, it can refer to specific components and services within that CSP's product space. For example, Linux in the IaaS category, Oracle as a service in the PaaS category, or Office 365 in the SaaS category.

In this section, we offer a concise subset of vendor cloud service offerings that are mature technologies and have been granted provisional authority by the FedRAMP Joint Authorization Board, as well as meeting other criteria potentially required by DoD cloud systems.

As of the current writing of this white paper, there are a total of 167 FedRAMP Ready, In Process, and Authorized products. Table 3 breaks this down with successively more restrictive filters. This shows that, while there are many FedRAMP authorizations, those that offer IaaS and PaaS, are baselined at FedRAMP High, and have a JAB P-ATO comprise a much smaller subset.

Table 3 - Applying successive filters to FedRAMP authorizations results in a smaller subset of products.

Filter	Count
All FedRAMP products (no filter)	167
Those with an <i>Authorized status</i>	89
Those with JAB authorization	29
Those with a Government Community Cloud deployment model	20
Those authorized to process data at the high impact level	3
Those that provide <i>both IaaS and PaaS</i>	2

Figure 4 shows the screen capture from the results in the filter results in Table 3. Both Amazon Web Services (AWS) and Microsoft Azure Government have received JAB authorization to process data at the high impact level. These cloud service offerings were authorized on 21 June 2016 but were assessed by different independent assessors.





 AWS GovCloud High	IaaS PaaS	High	 FedRAMP Authorized	3 Authorizations
 Azure Government	IaaS PaaS	High	 FedRAMP Authorized	12 Authorizations

Figure 4 - Screen capture from marketplace.fedramp.gov product search shows the two filtered results. (Information current as of the date of this white paper.)

The number of authorizations on the right indicate the agency-authorizations that have been completed for that provider. As we mentioned previously, the JAB P-ATO refers to a third-party organization completing their assessment of the security controls in place for that provider. However, the agency must still perform their own authorization process before those cloud services can be used by programs within that agency.

3.6.1 AWS GovCloud High

The AWS P-ATO applies to the AWS GovCloud (US) Region, including Amazon Elastic Cloud Compute (EC2), Amazon Virtual Private Cloud (VPC), Amazon Simple Storage Service (S3), Amazon Identity and Access Management (IAM), and Amazon Elastic Block Store (EBS). Launched in 2011, the AWS GovCloud (US) is an isolated region designed to host sensitive workloads in the cloud. In addition to FedRAMP, AWS GovCloud (US) adheres to U.S. International Traffic in Arms Regulations (ITAR), Criminal Justice Information Services (CJIS) requirements, as well as Levels 2 and 4 for DoD systems.

3.6.2 Microsoft Azure Government

Azure Government infrastructure is provided by Microsoft Global Foundation Services (GFS), which has also achieved a FedRAMP JAB P-ATO supporting in-scope services, including Azure Active Directory. The following Microsoft services are FedRAMP Authorized and approved by the JAB: KeyVault, ExpressRoute, WebApps, Azure Site Recovery (ASR), Microsoft Azure Backup (MAB), Notification Hubs, Service Bus, StorSimple, Automation, Azure Resource Manager (ARM), Batch, Media Services, Policy Administration Services (PAS), Scheduler, Log Analytics, and Redis Cache. In addition, Microsoft has a DoD cloud (a region of Azure Government) that is Impact Level 5-approved for infrastructure, platform, and

productivity services (including Office 365).

3.6.3 Recommendations (Cloud Service Offerings)

BE recommends that the organization determine the impact level of the data and an initial assessment of the required cloud service offerings. Then, start with the FedRAMP product list and determine the candidate providers. Next, examine the agency authorizations and determine which can be leveraged to yield the most satisfactory path for a system ATO. Finally, determine any additional and approved platform and software offerings provided by each vendor that add value to the cloud migration effort.

For services that are not available in the selected CSP's cloud offerings, BE recommends that the organization engage with industry and any specific vendors as demand drives vendors to offer services within government clouds.

4. Conclusion

This short white paper canvased, at a high level, what we believe to be the over-arching strategic security elements for DoD cloud migrations. The security concerns we have discussed here include the FedRAMP process and the FISMA data impact levels; the shared responsibility above and beyond the FedRAMP-mandated controls; the aspects of user access, authentication, and authorization; the planning for the STIG process; the different types of cloud service models; and finally, specific cloud service providers that have achieved the level of authorization typically required by DoD systems.

4.1 About Buchanan & Edwards (BE)

BE is an innovative, leading-edge technology solutions company with a 20-year record of helping federal clients meet mission-critical needs through high-quality personnel and technical solutions. Our over 350 personnel provide key support to national security, federal law enforcement, civilian, and intelligence agencies. We have experience implementing solutions in government clouds, using our partnerships with Amazon and Microsoft, where we have immediate provisioning ability on the Azure Government cloud within the FedRAMP High boundary.

We use mature, tailored Agile processes to develop and integrate solutions successfully for other complex systems, such as the Federal Bureau of Investigation (FBI) Delta, where we consolidated 127+ data sources to support FBI's investigative and analysis purposes. Our support for the Marine Corps Recruiting Information Support System (MCRISS) program includes standing up the Marine Corps' first cloud-based development and test environment.

At BE, we help our customers get the most out of infrastructure transformation. We are a vendor-neutral integrator, and this diversity is our strength. We provide our customers objective and reliable advice on cloud migration strategy and security, helping to navigate the complex landscape of cloud service providers and models. We help our customers develop plans to rearchitect and reengineer applications to get the most value out of cloud computing.

5. Resources

This resources section lists selected documents and websites related to the content of this white paper.

5.1 Documents

[Department of Defense Cloud Connection Process Guide](#)

[DISA] Version 2 (March 2017)

[Department of Defense Cloud Computing Security Requirements Guide](#)

[DISA] Version 1, Release 3 (March 2017)

[DON Cloud Update, DON IT Conference 2016](#)

[Department of the Navy] (July 2016)

[Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53](#)

[NIST] Revision 4 (April 2013 – Includes Updates as of 2015-01-22)

[Cloud Security Information Impact Level Matrix](#)

[DoN CIO]

[DoD Cloud Assessment Process](#)

[DoD CIO] (January 2015)

(This document references an older release of the CCSRG)

[Defending DoD Missions in the Commercial Cloud](#)

[Peter Dinsmore – DISA] (June 2015)

5.2 Websites

[FedRAMP Authorized Products](#)

[U.S. Government]

[AWS GovCloud \(US\)](#)

[Amazon]

[Department of Defense in Azure Government](#)

[Microsoft] (May 2017)

[Joint Regional Security Stacks \(JRSS\)](#)

[DISA]