UNITED STATES ARMY

USAASC

ACQUISITION SUPPORT CENTER

# USAASC Cloud White Paper

## August 2020



# TABLE OF CONTENTS

## List of Figures

# 1 EXECUTIVE SUMMARY

Following Department of Defense (DoD) guidance, in June 2014, the Secretary of the Army directed the migration of Army enterprise systems and applications to enduring data centers by the end of fiscal year (FY) 2018. Driven by this requirement and seeing the potential to significantly reduce costs and add flexibility, the U.S. Army Acquisition Support Center (USAASC) began investigating the use of a commercial cloud environment for its information technology (IT) systems portfolio. Migration to a cloud environment enables organizations to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while reducing hosting costs, improving continuity of operations, and increasing security. At that time, there was limited information available, within the Army and the larger DoD, on a clearly defined process to help organizations migrate to a commercial cloud environment.

Throughout its IT system cloud migration efforts, USAASC has worked closely with stakeholders across DoD and the Army to execute a sustainable transition to the cloud environment. USAASC successfully transitioned its Career Acquisition Management Portal/Career Acquisition Personnel and Position Management Information System (CAMP/CAPPMIS) from a traditional data center to the commercial Amazon Web Services (AWS) GovCloud environment in April 2020.

This paper is intended to support sharing key take-aways based on lessons learned for the migration from a traditional government data center to a commercial cloud environment for a Cloud Computing Security Requirements Guide (CC SRG) Impact Level (IL) 4 system. IL 4 computing environments are certified to handle personally identifiable information and sensitive information. The lessons learned are based on USAASC's migration of the CAMP/CAPPMIS to the commercial AWS GovCloud environment.

Critical take-aways are summarized below. Further details are provided in the subsequent sections of this paper.

- Conducting the Cost Benefit Analysis (CBA) requires a thorough understanding of the system to accurately estimate compute resource needs (e.g. number of instances, storage requirements, network throughput, etc.). When possible, a proof of concept should be performed in the targeted Cloud Service Provider (CSP) environment to help the team validate assumptions and accurately evaluate alternative commercial CSPs (Section 4.0).
- Government should procure cloud infrastructure resources separately and not as part of its System Integrator's (SI) Other Direct Costs (ODC) line. In the case of the latter, the root account credentials and overall security posture may fall solely under the contractor's purview and may introduce significant risk to government (Section 5.0).
- The new cloud environment may require services from an approved Cybersecurity Service Provider (CSSP) for endpoint security and vulnerability scanning tools. The majority of the tools configuration and customization will be the responsibility of the system owner and the designated system administrator(s) (Section 6.0).
- The IT system design should be established well in advance and based on unique system requirements, not default commercial CSP settings. The latter approach may introduce unnecessary dependencies on the infrastructure and result in extensive rework in the future if the system needs to be migrated to another CSP (Section 7.0).

- The IT portfolio system will require a new Authorization to Operate (ATO) prior to go-live in the new cloud environment. Due to limited familiarity with cloud technologies across government organizations, it is strongly recommended to establish and maintain close coordination with all parties by performing additional checkpoints and to gain consensus upfront on the strategy for the Enterprise Mission Assurance Support Service (eMASS) package (Section 8.0).
- Conducting pre-migration tests of the available data migration options will help determine the best one to utilize and support migration of the IT portfolio's high-priority applications and/or environments first (Section 9.0).
- Throughout the final cut-over activities, frequent sync meetings with government stakeholders are advisable to provide progress updates, address any issues or risks, and receive any feedback from the user community. A formal gate review should be conducted to officially transition the infrastructure to sustainment. These activities should identify any open findings, risks/issues, or actions needed for a successful transition (Section 10.0).

For further questions or guidance beyond the information presented, please reach out to the points of contact (POC) listed in Section 12 of this document.

# 2 PURPOSE AND INTENDED AUDIENCE

The purpose of this white paper is to share insights, key take-aways, and lessons learned from engagements with key stakeholders during USAASC's migration of CAMP/CAPPMIS from a traditional Army data center to a commercial cloud infrastructure.

The intended audience includes Army organizations that are currently hosted in a traditional government data center and want to learn about experiences from others across the Army that have migrated to a commercial cloud environment.

Note: The process documented in this paper is not necessarily the most current process. Please consult the Enterprise Cloud Management Office (ECMO) prior to beginning your migration.

# 3 CLOUD MIGRATION PROCESS OVERVIEW

The commercial cloud migration process (Figure 1) offers an outline for cloud migration phases, from cloud migration initiation to the final cut-over, and identifies the key phases (e.g., cloud migration) and major steps (bulleted list) based on USAASC's migration project. The section identified in parentheses outlines the key lessons learned that align with each phase.

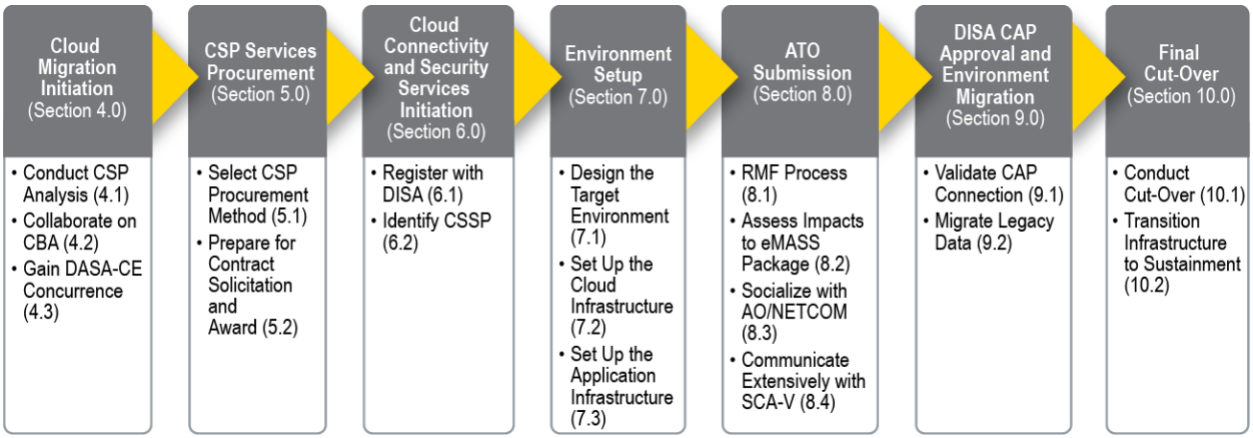



*Figure 1: USAASC Migration Phases*

## 3.1 Key Stakeholders and Roles

Throughout the migration process, USAASC collaborated with several Army and DoD-level organizations to obtain concurrence in support of migrating to a commercial cloud environment. The organizations and their specific roles in the migration process are listed below:

- Army Application Migration Business Office (AAMBO) was responsible for the initial cloud readiness assessment, CBA assistance and as a liaison between the application owner and the DoD-approved enterprise environment providers. In November 2019, this office became part of ECMO, which serves as the centralized, dedicated enterprise cloud migration resource for Army data and application owners (building cloud environments, architecture, contracting, resourcing, cloud and data migrations, cybersecurity, business case analysis, and industry best practices) to enhance speed, effectiveness, and efficiency of migrations to a cloud hosting environment.
- Chief Information Officer/G-6 (CIO/G-6) is responsible for application migration and data center consolidation policy and provides concurrence on CBA submissions.
- Deputy Assistant Secretary of the Army for Cost and Economics (DASA-CE) reviews and may provide final concurrence for the CBA.
- Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology's (ASA(ALT))/Office of the Chief Systems Engineer is responsible for the overarching cybersecurity for USAASC and contributes to the Risk Management Framework (RMF) and authorization process through the Authorizing Official (AO) and the Program-Information System Security Manager (P-ISSM) roles.
- System or application owner is responsible for application rationalization, CBA, CSP procurement, CSSP agreements, environment setup and migration, obtaining ATO, final cut-over and sustainment on cloud.
- Defense Information Systems Agency (DISA) registers the migrated system and provides access to a cloud access point (CAP). A CAP is needed for all IL 4 or 5 cloud environments to connect to the DoD network.
- The U.S. Army Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center is the CSSP. It provides Host-Based

Security System (HBSS) and Assured Compliance Assessment Solution (ACAS) licenses to track vulnerabilities within the USAASC IT system environment.

## 3.2 USAASC Cloud Migration Timeline

USAASC's migration to a commercial cloud environment spanned several years, as shown in Figure 2. For additional background, it is important to note the following key milestones that influenced the timeline:

- Following DoD guidance, in June 2014, Secretary of the Army directed the migration of Army enterprise systems and applications to core data centers by the end of FY18. In July 2015, the Army CIO/G-6 provided guidance for the migration of enterprise applications to the commercial cloud.
- Between August and October of 2015, USAASC completed the migration survey provided by AAMBO. On November 20, 2015, AAMBO delivered version 1.0 of its migration assessment and rough order of magnitude (ROM) of the CAMP environment and recommended that it move to the DISA hosting services.
- At the beginning of calendar year 2016, USAASC requested assistance from Acquisition Management Support Solutions (AMS2) to leverage their migration efforts for an analysis of alternatives (AoA) and proof of concept to validate AAMBO's recommendation.
- With the approval of the CAMP/CAPPMIS CBA in April 2018 (HQDA G-6 Memo Subject: Review of Data Center Migration CBA for Career Acquisition Management Portal [CAMP] to a Department of Defense Approved Enterprise Facility [DoDEF], C-BA CIO/G-6 No. 6307), USAASC allocated funding to complete its migration.
- Upon receipt of funding for the migration, USAASC engaged with AMS2 in 2018 to initiate the effort.

To summarize the efforts, the milestones are grouped into four key categories, as shown in the Figure 2 legend:

- Contract
- Cyber
- Process
- Technical

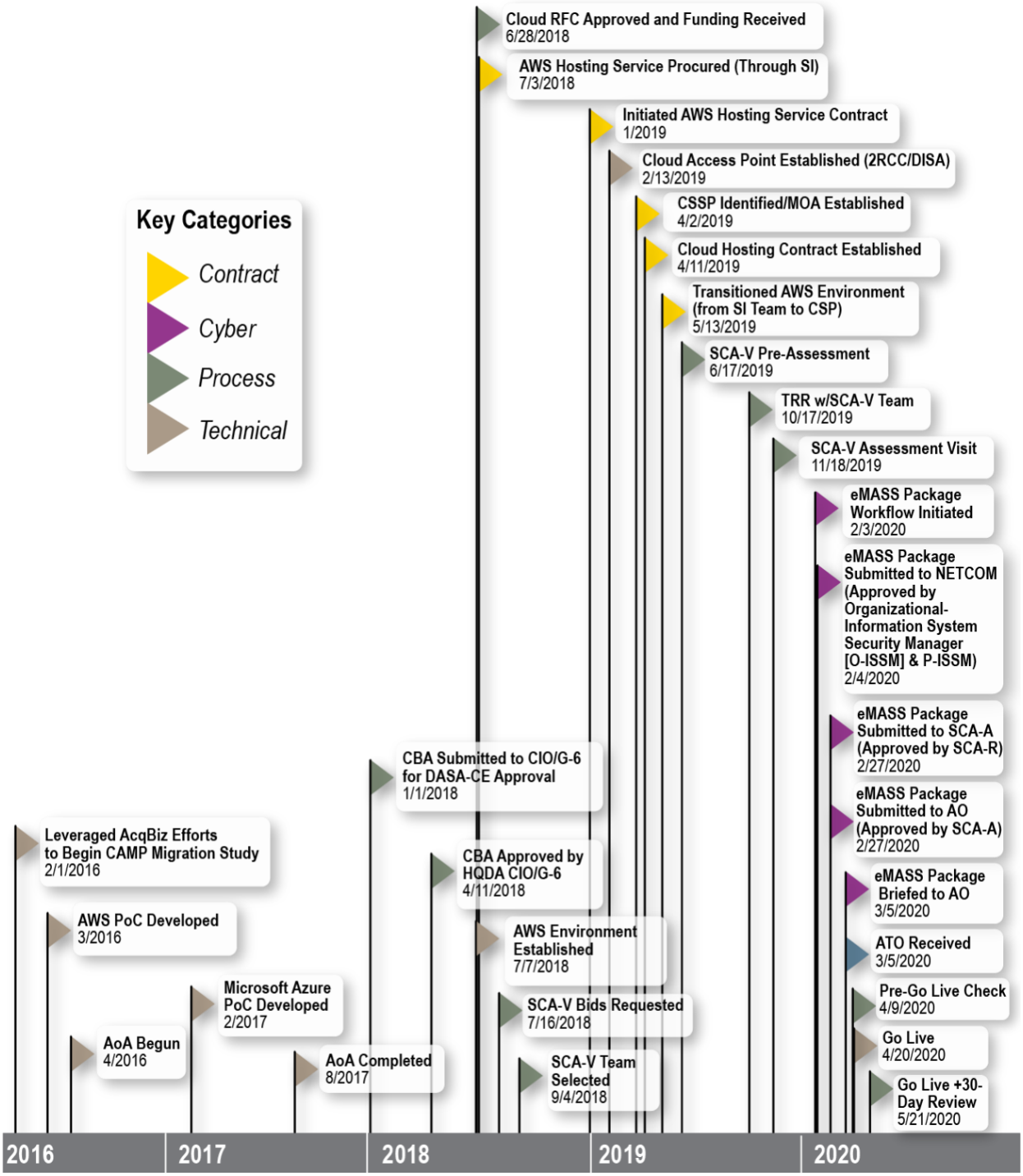
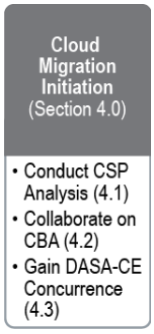



*Figure 2: Cloud Migration Timeline*

Over the past FY, the major milestones that illustrated significant events for the USAASC cloud migration effort include:

- Go Live: April 20, 2020
- ATO Received: March 5, 2020
- Security Control Assessment-Validation (SCA-V) Visit: November 2019

# 4 CLOUD MIGRATION INITIATION




Upon initiation of the USAASC cloud migration, the Army lacked formal guidance and a detailed process guide was not available. It is worth noting that ECMO (as mentioned in Section 3.1) was established in November 2019 within the Office of the CIO/G-6. This office was stood up toward the end of the CAMP/CAPPMIS cloud migrations, and as a result, USAASC did not get a chance to engage directly with ECMO. Going forward, this is a key resource for future Army cloud migration efforts. A link to ECMO's Cloud 101 brief can be found here. Please note that references made in Section 4 below pertaining to ECMO occurred with AAMBO when AAMBO was a stand-alone organization. Coordination going forward should occur directly with ECMO. In this coordination, it is essential that Army organizations identify all approving authorities and key stakeholders, and understand the high-level processes for migration prior to initiation.

## 4.1 Conduct CSP Analysis

**Key Take-Aways: Cloud Migration Initiation**

- ✓ Identify key stakeholders and roles (see Section 3.1) and the corresponding POC and information within each organization.
- ✓ Stay in lockstep with ECMO for consensus before presenting CBA results. Ensure that any recommendations for the target environment are closely coordinated with ECMO.
- ✓ Cost estimates should be developed using calculators provided by the commercial Cloud Service Provider on its website (e.g., Amazon GovCloud, Microsoft Azure).
- ✓ The IT system's design should be established well in advance and based on unique system requirements, not default or template settings.

Before proceeding with the CBA, organizations must conduct a comprehensive AoA in partnership with ECMO to assess all available cloud service offerings and to identify the best-fit solution for system and application portfolio hosting needs.

The CSP evaluation begins with an analysis of all infrastructure as a service (IaaS) and platform as a service (PaaS) offerings in the DoD Cloud Service Catalog. Options that do not meet the initial criteria should be eliminated. Examples of characteristics that make an option unusable may be the lack of a current Cloud Computing Security Requirements Guide Provisional Authority (CC SRG PA), or the inability to support the desired target cloud architecture.

Although a template and high-level scoring guidance were provided by DASA-CE to help evaluate the various CSP options, USAASC identified an additional 10-point scale based on the following criteria:

- Cloud capabilities
- Security
- Ease of migration
- Management and monitoring
- Disaster recovery/continuity of operations (COOP)
- Service-level agreements (SLAs)
- Consumption model
- Governance, risk management, and compliance

In addition to the AoA, USAASC conducted proofs of concepts in the targeted CSP environments to help the team validate assumptions and accurately evaluate alternative commercial CSPs. Time and resources permitting, this would provide several benefits, including validating assumptions, helping identify risks/issues to be explored further, and providing

additional justification to support the final recommendation. For example, the SI team initially had considered the Microsoft Azure PaaS offering; it was only during the proof of concept that they validated it was not feasible because of cross-database querying constraints.

In conducting the CSP analysis, it is important to accurately estimate the computing resources, number of instances, storage requirements, and network throughput cost using calculators available on the CSP websites. In addition, system design should be established well in advance and based on unique system requirements, not default commercial CSP settings. This will ensure that the system implementation is not reliant on any specific cloud service provider's services.

## 4.2 Collaborate on CBA

Once complete, the organization should coordinate with both ECMO and CIO/G-6 for consensus on the CBA results and recommendations before presentation to DASA-CE. In addition, ECMO will assess the system's hosting requirements and current system configuration to perform an independent assessment and provide recommendations to DASA-CE and CIO/G-6. As a result, system owners should coordinate closely with ECMO on desired outcomes.

## 4.3 Gain DASA-CE Concurrence

DASA-CE requires that CBA submittals use the template and spreadsheet listed below:

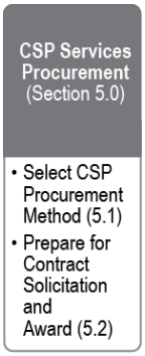
- CBA briefing using DASA-CE template
- Cost element structure (CES) spreadsheet: CES must include estimates of key costs related to hosting over 10 years, initial migration cost, and sensitivity analysis.

In addition, a lifecycle cost estimate (LCCE) is required. The LCCE should be made based on well-defined, system-specific hosting requirements and estimate the projected hosting costs over the next 3 years. In conducting the CBA, to ensure accurate estimation of the computing resources, number of instances, storage requirements, and network throughput costs, use the calculators available on the respective CSP websites.

Once concurred with, DASA-CE will provide documented consent on the CBA findings and recommendation. This is required to proceed in the cloud migration process.

# 5 CSP SERVICES PROCUREMENT

Ahead of the CSP services procurement process, Army organizations should identify all possible commercial cloud procurement options and actively engage with their government contracting agency, keeping in mind that procurement time from the start to final award may take several months.




## 5.1 Select CSP Procurement Method

To acquire CSP services, there are two options potentially available for procurement of the cloud infrastructure resources:

1) Engage the Army or DoD contracting office to identify and secure a contract vehicle for the cloud hosting services via a new solicitation or the use of an existing contract: strongly recommended.
2) Use ODC funds for procurement.

Use of the ODC funding via the same contract used for the SI team services is not recommended, for several reasons. USAASC chose to compete a separate hosting contract after careful consideration of the issues below:

- Environment and root account credentials may not be controlled by the government, depending on the type of setup and configuration provided by the contractor. This also means that any data or information loaded into the environment may not be exclusively controlled by the government, and that the contractor may be responsible for some or all security postures.
- Environment also depends on the availability of that specific contract. This means if the Army organization recompetes the SI contract and the incumbent loses, the government could lose access to the cloud infrastructure. In the event of award to a new SI team, the existing infrastructure may need to be rebuilt from the ground up or transitioned to the new SI contractor's environments.
- CSP bills at least 1 month in arrears, so immediate funding status is not available or visible. For example, usage for April 2019 will not be billed to the contractor until mid-May 2019, and the contractor does not reflect disbursement until June 2019, 2 months after usage. This makes it harder to track the exact remaining funding on the ODC line.

**Key Take-Aways: CSP Services Procurement**

- ✓ Government should procure cloud infrastructure resources separately and not as part of the SI/contractor's ODC line.
- ✓ Establish clearly defined roles, responsibilities for performing the migration via an MOA or SIA if ODC funding via SI contractor is the only option.
- ✓ Development of PWS requirements and resources will help accurately evaluate the vendor and corresponding costs.

However, in the event that ODC funding is considered to be the only option, Army organizations should explicitly document roles and responsibilities with the contractor—especially in case of transition to another contractor. A memorandum of agreement (MOA) or system interface agreement (SIA) should be in place to define ownership, security, and responsibilities between government and contractor.

## 5.2 Prepare for Contract Solicitation and Award

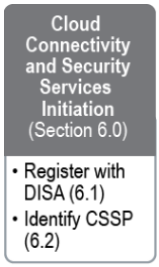
Prior to engagement with a DoD Contracting Office to identify and secure a contract vehicle for the cloud hosting services, it is recommended to go through ECMO for consultation. For contract solicitation, ECMO advises Army organizations as they acquire CSP services with one of several cloud contract vehicles. ECMO has also advertised that in the future, an ECMO-provided CSP reseller contract will be available for use.

Army organizations may also work with a government contracting agency to develop guidelines for performance work statements (PWS), as USAASC did. These guidelines identify specific requirements related to security, financial-management reporting, alerts-management reporting, and resource provisioning, including requirements that need dynamic scaling of the infrastructure. The PWS should also specify anticipated resources for the system baseline (e.g., licenses, central processing using (CPU), memory, data transfer, and attached storage). Determining all requirements and resources will help accurately evaluate the vendor costs.

# 6 CLOUD CONNECTIVITY & SECURITY SERVICES INITIATION

## 6.1 Register with DISA

To connect IL 4 and 5 applications to approved cloud environments, system owners must first request connection approval from DISA's Cloud Services Support Office (CSSO). CSSO maintains a formal process to obtain this permission, described in the "DoD Cloud Connection Process Guide." To initiate the process, the system owner must complete a DoD cloud information technology project (C-ITP) registration and connection form and obtain a cloud permission to connect (CPTC) memorandum. All requested documentation must be provided during registration, or the request will be kicked back.




Once registration has been processed and a CPTC memo is in hand, connection to the CAP can be achieved. The CAP is the security conduit through which DoD connects to the commercial cloud.

One of the required artifacts for DISA registration is the system's ATO. USAASC was able to leverage the existing ATO for its system located at the legacy host data center to initiate initial connectivity to the CAP. DISA was then provided the new ATO once it was received several months later. This allowed USAASC to work on the CAP connectivity configurations prior to receiving the new ATO and to troubleshoot issues far in advance of go-live.

During this initial connectivity period, DISA will provide the system administrators with specific instructions for CAP connection configuration. If needed, DISA will help troubleshoot to ensure that traffic is flowing as expected. After these initial tests are completed and successful, it is the responsibility of the system administrators to apply the correct configurations and enable access to the system through the AWS virtual private cloud (VPC) console.

**Key Take-Aways: Cloud Connectivity & Security Services Initiation**

- ✓ Army organizations will need to address the CSSP role in transitioning to a commercial cloud environment.
- ✓ System administrators will be required to complete DISA and CSSP required training in order to gain access to HBSS and ACAS. This is a hard requirement; the CSSP will grant access accounts only when the certificates for the required classes are submitted. As the CSSP only supplies and maintains the tools, the system administrators will be responsible for configuring and implementing.
- ✓ Enforcement of full policies may adversely impact system operations and requires in-depth troubleshooting for system administrators to implement policy and configuration exceptions to allow intended system functionality.

## 6.2 Identify CSSP

In addition to DISA registration, the cloud system must obtain services from an approved CSSP, which provides endpoint security (HBSS) and vulnerability scanning (ACAS). While traditional Army data centers include HBSS and ACAS in their hosting services, commercial cloud providers do not include these, and the system owner is responsible for installation, configuration, and execution of HBSS and ACAS.

It is important to remain proactive in coordinating with the CSSP to get all services configured and functioning properly. Full configuration is a multi-step, complex process that requires support from multiple teams within the CSSP. Documentation was not readily available, and constant discussions with the CSSP owner and their technical POCs best supported the

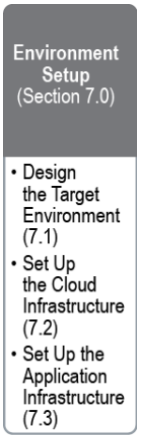
configuration. It is best to have a representative from the CSSP participate in all coordination meetings leading up to and during the SCA-V and to continuously ask "what's next" in order to move through the entire configuration process.

The CSSP provides endpoint security via HBSS, which is required to monitor, detect, and defend the new cloud environment. The CSSP provides baseline configurations only for all endpoint products. Installation and customization are the responsibility of the system administrators. The administrators must ensure that endpoint products are installed on all required assets and must customize the policies and exceptions. It is important to note that fully enforcing all policies could adversely affect system functionality. Prior to obtaining access to the CSSP-provided HBSS solution, administrators must complete DISA HBSS training, which consists of two courses, each 30 hours in length.

The CSSP also provides vulnerability scanning via ACAS, which is required to monitor, detect, and defend the new cloud environment network and systems. The CSSP only provides a server image and configuration documentation for the ACAS server to be deployed within the environment's demilitarized zone (DMZ). Installation and configuration of agents are the responsibility of the system administrators. These administrators must ensure full connectivity for all servers, as well as create and maintain credentials for the ACAS server to utilize to scan the system. Prior to obtaining access to the CSSP-provided ACAS solution, administrators must complete DISA ACAS training, which consists of a 40-hour course.

# 7 ENVIRONMENT SETUP

## 7.1 Design the Target Environment




To ensure a smooth and successful cloud migration, the architecture needs to be well designed from the start. As mentioned in Section 4.2, be sure that the design and configuration are tailored for the unique requirements of the Army organization's system and are not solely reliant on the inherent commercial cloud configurations. Some of these default configurations cannot be changed once they are implemented without large amounts of rework required within the environment.

Cloud migration strategies vary, but a best practice is to create the infrastructure in the cloud environment before migrating applications and data. This strategy can be utilized in most application migrations, unless the application is containerized and includes its own infrastructure within the container. For increased efficiencies, CSP-provided machine images may be used to initiate the first elastic compute cloud (EC2) instance before applying all necessary patches, security agents, DoD Security Technical Implementation Guides (STIGs), and clone instance, and proceeding with application infrastructure software installations. The most efficient cloud migration strategy is based on copying or cloning of baselined instances. Initial baseline should include patched and configured operating systems. Final baseline should include installed and configured application infrastructure with all CSSP security components.

**Key Take-Aways: Environment Setup**

- ✓ System design should be established well in advance and be based on unique system requirements, not default or template settings.
- ✓ Perform assessment to identify gaps in new environment (e.g., need for system administrators, software licenses).
- ✓ Test networking settings and configurations prior to final cut-over, utilizing "dummy" access to the cloud environment.
- ✓ Identify software baseline well in advance and allocate necessary time for the procurement of any software licenses.

## 7.2 Set Up the Cloud Infrastructure

System architectures of cloud environments depend on requirements, but the best practice is to create separate VPCs. Non-production environments, including development and test, should reside in separate VPCs. Production environments should be isolated to their respective VPCs and should include the development perimeter network or DMZ, security VPC, and Shared Services. This architecture provides the highest security, as the two environments will be in separate VPCs. Main and backup application controllers like an F5 should be set up to control environment and application access.

USAASC experienced challenges in accessing the AWS GovCloud environment via the F5 Virtual Private Network (VPN), which had been securely configured using the military unique deployment guide (MUDH). The F5 VPN conflicted with both the contractor VPN on contractor laptops and the Fort Belvoir VPN on government furnished equipment (GFE) laptops. As a workaround, VirtualBox virtual machines (VMs) were used to access the cloud environment, which ultimately proved to be beneficial for contractor laptops. However, a different approach was required for GFE devices. A separate VPN connectivity profile or additional installation executable must be made available or installed on the GFE devices by the appropriate administrative groups. As this is not a well-documented process for new cloud environments, consideration should be given to begin this process as early as

possible once the final VPN solution has been identified. Networking settings and configurations should be tested prior to final cut-over, utilizing "dummy" access to the cloud environment. This allows testing of the domain name server (DNS)/routing/networking configuration settings in advance and provides additional time to troubleshoot with Second Regional Cyber Center (2RCC) and DISA should any issues arise.

Public key infrastructure-equipment (PKI-E) certificates are required to be installed on all servers and must be requested from an approved DoD source. In order to request these certificates, the requesting organization must have an appointed trusted agent (P-ISSM), delegated agent (Information System Security Officer [ISSO]), and server administrator (system administrator). The official PKI-E portal has all required instructions and templates to have individuals appointed and to request and install certificates.

Requesting and obtaining administrator tokens turned out to be a very lengthy process. Although a cloud infrastructure allows system administrators to access the system from disparate geographic locations, in-person pickup of the tokens is required at Fort Belvoir, or whichever DoD location they are requested from. Once the tokens are issued, a technical solution for keeping the tokens active has been an ongoing challenge. Any user requesting an administrator token must comply with DoD and Army requirements for privileged users (DoD 8570.01-M and DoDD 8140.01).

## 7.3 Set Up the Application Infrastructure

The process to set up application infrastructure (for most systems) should start with software installation on baselined cloud instances in development environments. Afterward, baselined and configured images can be cloned to create test and production environments.

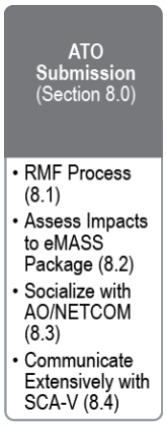
After software installation and configuration, all necessary ports should be configured and communications between infrastructure components validated. In addition, elastic internet protocols (IPs) should be assigned to the appropriate cloud instances to reserve static IPs, such as database servers and web servers. Once the application infrastructure for development environments is validated, it can be cloned to test and production environments. In each environment, IPs should be assigned to instances and environment-specific configurations completed before performing application migration.

Obtaining software licenses is also a very lengthy process, so ensure that enough time is allocated for these procurement activities to occur. Determine the software baseline well in advance in order to finalize the system design, allow for time to procure any new licenses needed, and account for any delays in processing or technical issues.

# 8 ATO SUBMISSION

## 8.1 RMF Process

The standard Army RMF process must be followed to receive an ATO for the new cloud environment. The U.S. Army Network Enterprise Technology Command (NETCOM) tactics, techniques, and procedures (TTP) documents should be consulted for guidance on navigating through the process.




## 8.2 Assess Impacts to eMASS Package

Impact to the eMASS package should be assessed and documented upfront to include identification of any inherited controls, applicable STIGs, and development of all new test results specific to the cloud environment of the Army organization. Some of these test results may not change at all from the legacy system to the cloud, and others will change drastically. Regardless, each must be reviewed and updated as required.

After determining the appropriate option to take with the eMASS package, ensure that a new categorization worksheet is complete, and then update and receive approval of the Security Plan. This will ensure that data types and resulting confidentiality, integrity, and availability (CIA) levels are accurate. Within the eMASS package, inherited controls must be addressed and might not be as straightforward as expected, depending on the Army organization's CSP and CSSP. Currently, the AWS GovCloud IaaS (IL 4) eMASS record does not have a traditional ATO; rather it has a provisional authorization based on its Federal Risk and Authorization Management Program (FedRAMP) approval. Inheritable controls are available, and they contain applicable test results. C5ISR does not currently have an eMASS package. Therefore, controls being inherited from C5ISR as part of its CSSP services must be manually identified and agreed upon. Every system has its own unique circumstances; different CSPs and CSSPs may or may not have approved eMASS packages, as things are constantly changing and adapting. It is advisable to address these factors as they apply to the system early in the RMF process to prevent unplanned delays as progress is made.

**Key Take-Aways: ATO Submission and DISA CAP Approval**

- ✓ Socialize plan to migrate to the cloud with AO and NETCOM to obtain consensus on path forward.
- ✓ Conduct a "Pre-Assessment" with the SCA-V team approximately 6 months prior to the official assessment.
- ✓ To prepare for the SCA-V assessment, all STIG checklists for applicable technologies should be completed on applicable servers, to include all manual checks.

Test results must then be written for these controls which reference the specific section and page number of the signed agreement with them. This signed agreement becomes a very important artifact to ensure that all requirements are accounted for and have the correct responsible entity. All supporting system documentation must also be updated. It is imperative to remove any references to the previous on-premise data center to eliminate any confusion. The system documentation should also contain detailed descriptions of the processes and/or configurations and should do more than just restate the assessment procedures. Once all system documentation has been updated, and prior to the SCA-V assessment, it should be reviewed and signed by government leadership of the Army organization.

## 8.3 Socialize with AO/NETCOM

It is highly recommended to socialize the plan to migrate to the cloud with the Army organization's AO and NETCOM well in advance to get buy-in on the way forward. Details on scheduling/timing, eMASS package, or other unique requirements should be worked out at this time, which will minimize delays moving forward through the RMF process. Specifically related to planning the eMASS package, there are multiple approaches to be considered as far as completing the package for the new cloud system. It is possible to update the system's existing eMASS record with the new cloud information; however, this may cause confusion with maintaining the legacy system while updating for the new cloud system. It is also possible to create a new, separate eMASS record for the cloud system. This allows for clearer separation between the new and legacy systems, but also requires the update and maintenance of two packages simultaneously until the cloud migration is finalized. These factors should be considered in consultation with the AO of the Army organization and NETCOM to determine the best path forward.

## 8.4 Communicate Extensively with SCA-V

Extensive communication and coordination with the SCA-V team throughout the entire process is paramount in completing a successful assessment. Some recommendations on explicit sync sessions are listed below:

- Schedule a "pre-assessment" with the SCA-V team approximately 6 months prior to the official assessment. This gives the SCA-V team an opportunity to provide feedback on the current technical status of the cloud environment, review system documentation, and provide any recommendations. It also provides a buffer in case any of the issues mentioned above are not fully resolved. The SCA-V "pre-assessment" is a good opportunity to review these new test results with the SCA-V team and receive feedback.
- Schedule an integrated product team (IPT) meeting to include the SI, SCA-V team, CSSP, and any government stakeholders to review accomplishments, roadblocks, and next steps. IPT meetings, including the SCA-V team, should begin to take place weekly after the pre-assessment has taken place up until the SCA-V assessment. This will ensure that the SCA-V team is tracking progress and can provide recommendations prior to the SCA-V assessment.
- Typically, the SCA-V team holds a Technical Readiness Review (TRR) meeting about 1 month prior to the official SCA-V assessment. Since the cloud technologies are relatively new and the application of their existing processes and requirements can vary, discuss the cloud environment and ensure consensus on the significant differences and resulting impacts on traditional requirements during TRR. For example, on-premise data centers require COOP; however, commercial cloud service providers have inherently built redundancies within their architectures, so a separate "hot/cold" or "hot/hot" site is no longer needed.
- It is also critical to gain concurrence on the impacts to the eMASS package. For example, gaining consensus on the handling of inheritance and test results should be addressed upfront. As mentioned in Section 8.2, the different CSPs and CSSPs have their own eMASS packages with varying types of authorizations and amounts of

inheritable controls. Based on your specific CSP and CSSP, the approach for completing your eMASS package could require additional coordination.

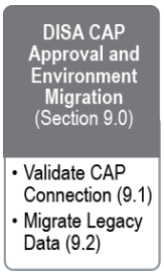
- In addition to the SCA-V's required TRR, it is helpful to have an additional follow-up meeting approximately 2 weeks prior to the SCA-V assessment. This allows both sides to follow up on questions and review the status of actions identified during the TRR. USAASC provided the SCA-V team with a detailed agenda for each meeting and followed up with notes and actions documenting discussion topics, decisions, and meeting outcomes.
- Heading into the formal SCA-V assessment, USAASC collaborated with the SCA-V team to define an initial agenda for the week of the SCA-V assessment, including the technology POCs and system administrators for each technology and proposed times/durations for review.
- During the week of the assessment (pre- or official), it is very important to make sure that all personnel are fully engaged and available to support. If there are specific times that people are not readily available, it should be communicated upfront on the proposed agenda/schedule. Depending on the size of the Army organization's team, having multiple conference rooms or private work areas available for breakout sessions can be very helpful. In the case that large rooms are being shared, it is beneficial to have similar/related technologies reviewed in the same room (e.g., Red Hat Enterprise Linux (RHEL) and Apache), which allows for easy collaboration when needed.
- To prepare for the SCA-V assessment, all STIG checklists for applicable technologies should be completed on applicable servers, including all manual checks. System administrators should ensure that the most recent versions are being used from the cyber.mil website, and that all their supporting system documentation and/or notes are available for reference.

As mentioned in Section 6.1, USAASC also found it very beneficial to have a representative from the CSSP participate in all coordination meetings leading up to the SCA-V, as well as being on-site for the assessment. This allows them the opportunity to accurately describe their role in supporting the system and for quick reach back to their organization if needed.

After the official SCA-V assessment, the team should immediately start remediating open findings while waiting for the final SCA-V report. This will allow for a quicker turnaround in submitting the final eMASS package for approval after the final report is received. Utilize the STIG checklist files that were completed during the assessment, as those will be uploaded into eMASS by the SCA-V team. Ensure that the remediation actions are closely tracked for all technologies and applicable servers, and that supporting evidence is created to maintain an accurate record of what has been done. Once the final SCA-V report is received, allow ample time (this could take several weeks) to continue addressing findings and completing plan of actions & milestones (POA&M) until an acceptable security posture is reached for finalizing the eMASS package and moving forward with submission.

# 9 DISA CAP APPROVAL & ENVIRONMENT MIGRATION

## 9.1 Validate CAP Connection




Once the ATO is received, the DoD C-ITP registration, which was completed during the initial DISA registration, should be updated with the new ATO and expiration date, along with any other system documentation that has been updated. The initial CAP configuration completed earlier in the migration process should enable this final connection process to occur in a timely manner. Coordination with DISA is required to help troubleshoot the connection, and the CAP connection must be thoroughly tested at this point to confirm that all aspects of the system can operate correctly. After connection to the CAP has been finalized, connectivity to external interfaces can be validated and final cut-over can be initiated.

After obtaining an ATO and connection to the CAP, the systems and applications in the legacy hosting environment can be decommissioned. Before decommissioning, the most up-to-date data must be migrated from the legacy to the cloud environment.

## 9.2 Migrate Legacy Data

Data sets may include database dump files, image files, user directories, and other files that are constantly updated.

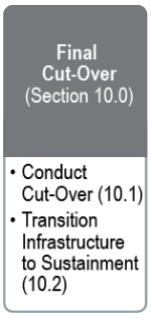
**Key Take-Aways: Environment Migration**

- ✓ Maintain access to the legacy system in order to compare software configurations to those in the cloud.
- ✓ Conduct pre-migration tests of the available migration options to help determine the best one to utilize.
- ✓ Coordinate with any external connections in advance to ensure all required updates to existing settings or processes are made.

There are a variety of options available for use in migrating the data from the legacy data center into the cloud. Deciding which one to utilize is based on a variety of factors and should be evaluated based on quantity of data, network speed, geographic location, DoD Security Requirements Guide (SRG) requirements for different ILs, timeline, and cost. Conduct pre-migration tests of the available options to help determine the best choice. If possible, it is best to evaluate if real-time connectivity can be utilized between the existing host data center and the cloud environment, which would alleviate the dependencies on travel and/or shipping of data storage devices. It would also permit real-time data transfer and minimize downtime. Conduct a trial run with a small subset of data prior to the final migration. This allows for the technical and procedural details to be worked out with the host data center ahead of time. It should also be noted that advanced coordination with any external connections or dependencies should be initiated months in advance to ensure that all required updates to existing settings or processes are made (e.g., DISA firewall exception updates).

# 10 FINAL CUT-OVER

Obtaining connection to the DISA CAP will make production systems and applications visible on the network; but to finalize the cut-over, certain steps must be performed to refresh data, validate external interfaces, and update the DNS to point to a new cloud environment. This process may require some downtime to stop updates on a system residing in the legacy environment, migrate data, and switch users to the cloud environment.




## 10.1 Conduct Cut-Over

Prior to the final cut-over, an acceptable migration window should be coordinated with government leadership and system stakeholders, and advanced notice should be given to end users of the anticipated downtime. To minimize downtime, detailed plans with estimated execution times, responsible POCs, and defined steps should be produced. High-priority applications and environments should be identified as well, as these will be the initial focus during the final cut-over. In most cases, high priority should be given to those applications or environments utilized by the largest number of end users (e.g., production environments).

**Key Take-Aways: Final Cut-Over**

- ✓ Coordinate an acceptable migration window with leadership and stakeholders.
- ✓ Identify high-priority applications and/or environments and migrate those first.
- ✓ Conduct daily sync with stakeholders to provide frequent updates and address any issues.

When completing the final cut-over, the identified high-priority applications or environments should be migrated first. This will ensure that a successful migration is accomplished in a timely fashion for a majority of the end users. Once that has been completed, then transition to the lower-priority applications or environments (e.g., development and/or testing environments). It is still helpful to maintain access to the legacy system at this point, as it allows for comparison of software configurations across the environments, and the ability to provide connectivity workarounds while the final migration processes are being completed. External interfaces must be updated and validated in the new cloud environment, then disconnected from the legacy environment. At the end of the cut-over process, DNS entries should be updated to point uniform resource locators (URL) to the new cloud environment.

## 10.2 Transition Infrastructure to Sustainment

Leading up to the final cut-over, conducting regular sync meetings with government stakeholders is recommended to provide regular progress updates, address any issues or risks, and receive any feedback from the user community. These meetings should occur leading up to, and then continue through the migration, as transition into sustainment begins.

Nearly a week prior to final cut-over, it is recommended to conduct a D-7 meeting to walk through the final migration checklist, review the timeline for migration and cut-over, provide a status on the final security posture of the system, and establish the communication cadence for the final stages of the migration and cut-over. This communication cadence during the cut-over should include daily checkpoints at which a status is provided and any issues are discussed.

About a month after the final cut-over, once the system has been operating out of the cloud, it is recommended to conduct a D+30 meeting to gain government consensus on any remaining

actions needed to successfully transition to sustainment. Similar to the D-7 meeting, stakeholders should review the migration timeline and what has been completed, provide a status on the current security posture of the system, and discuss any outstanding issues.

# 11 BENEFITS

Migrating a system to the cloud results in many benefits for the Army organization. To identify the true return on investment requires operating in the cloud for at least a full year. However, in the meantime, several benefits are readily apparent related to resources, technology, and operations.

From a resources perspective, CSPs bill only for actual consumption, resulting in a more efficient payment model for government organizations. The government recognizes financial savings during periods of low usage (e.g., weekends and holidays), and/or Army organizations can power off nonessential environments (e.g., development or test) when not in use to further reduce operating costs. CSPs also provide massive economies of scale by sharing computing environments across hundreds or thousands of customers, which translates to lower pay-as-you-go prices. In addition, cloud technology provides changes to the traditional contingency and alternate site procedures. Contingency procedures in the cloud are an automatic process that is conducted through redundancy. Therefore, funding and maintaining a physically separate alternate site is not required, which provides an additional cost savings. All actual incurred costs can be viewed in real-time, drill-down dashboards and reports.

From a technical standpoint, CSPs provide mechanisms to perform automatic upgrades of virtualized machines with zero downtime, enhancing the government's ability to quickly respond to security posture changes. CSPs also provide automated monitoring of all system resources, including IaaS and PaaS offerings. In addition, system administrators can implement "task-oriented alarms," which perform actions based on alert levels (e.g., spinning up additional servers to meet increased demand).

Operationally, CSPs allow for the rapid deployment of additional servers as new requirements emerge, such as new applications or features. The system owner maintains more control over resources and the implementation of its change management process, rather than relying on the host data center's approvals and processes.

# APPENDIX A: ACRONYM LIST

| ABBREVIATION | MEANING |
|---|---|
| 2RCC | Second Regional Cyber Center |
| A & A | Assessment & Authorization |
| AAMBO | Army Application Migration Business Office |
| ACAS | Assured Compliance Assessment Solution |
| AMS2 | Acquisition Management Support Solutions |
| AoA | Analysis of Alternatives |
| AO | Authorizing Official |

| | |
|---|---|
| ASA(ALT) | Assistant Secretary of the Army for Acquisition, Logistics, and Technology |
| ATO | Authorization to Operate |
| AWS | Amazon Web Services |
| C5ISR | Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance |
| CAMP/CAPPMIS | Career Acquisition Management Portal/Career Acquisition Personnel and Position Management Information System |
| CAP | Cloud Access Point |
| CBA | Cost Benefit Analysis |
| CC SRG | Cloud Computing Security Requirements Guide |
| CC SRG PA | Cloud Computing Security Requirements Guide Provisional Authority |
| CES | Cost Element Structure |
| CIA | Confidentiality, Integrity, Availability |
| CIO/G-6 | Chief Information Officer/G-6 |
| C-ITP | Cloud Information Technology Project |
| COOP | Continuity of Operations |
| COR | Contracting Officer's Representative |
| CPTC | Cloud Permission to Connect |
| CPU | Central Processing Unit |
| CSP | Cloud Service Provider |
| CSSO | Cloud Services Support Office |
| CSSP | Cybersecurity Service Provider |
| DASA-CE | Deputy Assistant Secretary of the Army for Cost and Economics |
| DISA | Defense Information Systems Agency |
| DMZ | Demilitarized Zone |
| DNS | Domain Name Server |
| DoD | Department of Defense |
| DoDEF | Department of Defense Approved Enterprise Facility |
| EC2 | Elastic Compute Cloud |
| ECMO | Enterprise Cloud Management Office |
| eMASS | Enterprise Mission Assurance Support Service |
| FedRAMP | Federal Risk and Authorization Management Program |
| FY | Fiscal Year |
| GFE | Government Furnished Equipment |
| HBSS | Host-Based Security System |
| HQDA | Headquarters, Department of the Army |
| IaaS | Infrastructure as a Service |
| IL | Impact Level |
| IMO | Information Management Officer |
| IP | Internet Protocol |
| IPT | Integrated Product Team |
| ISO | Information System Owner |
| ISSO | Information System Security Officer |

| | |
|---|---|
| IT | Information Technology |
| LCCE | Lifecycle Cost Estimate |
| MOA | Memorandum of Agreement |
| MUDH | Military Unique Development Guide |
| NETCOM | U.S. Army Network Enterprise Technology Command |
| ODC | Other Direct Costs |
| PaaS | Platform as a Service |
| P-ISSM | Program-Information System Security Manager |
| PKI-E | Public Key Infrastructure-Equipment |
| POA&M | Plan of Actions & Milestones |
| POC | Point of Contact |
| PWS | Performance Work Statement |
| RHEL | Red Hat Enterprise Linux |
| RMF | Risk Management Framework |
| ROM | Rough Order of Magnitude |
| SCA-V | Security Control Assessment-Validation |
| SI | System Integrator |
| SIA | System Interface Agreement |
| SLA | Service Level Agreement |
| SQL | Structured Query Language |
| SRG | Security Requirements Guide |
| STIG | Security Technical Implementation Guide |
| TRR | Technical Readiness Review |
| TTP | Tactics, Techniques, and Procedures |
| URL | Uniform Resource Locator |
| USAASC | U.S. Army Acquisition Support Center |
| VM | Virtual Machine |
| VPC | Virtual Private Cloud |
| VPN | Virtual Private Network |

# APPENDIX B: MILESTONE DURATION

Once initial communication has taken place with ECMO, it is essential to begin creating a high-level timeline by backward-planning based on how long ECMO advises the turnaround time is for major milestones. Army organizations should go into this migration knowing it takes years to complete rather than months. Based on USAASC's experience, high-level milestones from Figure 2 are shown below along with the time to completion. Durations shown below are estimates; Army organizations going through the migration may experience more or less time to complete.

| MILESTONE | DURATION | COMMENTS |
|---|---|---|
| Establish CSP hosting contract | ~120 days | |
| DISA registration | ~30 days | |

| | | |
|---|---|---|
| Establish CSSP and provided services | ~60-90 days | Required technical configuration can vary; completing required training could add more time |
| SCA-V bid request and selection | ~60 days | Begin process 6 months prior to desired assessment date |
| SCA-V pre-assessment | ~7 days | 6 months prior to official assessment |
| TRR with SCA-V | 1 day | 30 days prior to official assessment |
| SCA-V assessment (official) | ~7 days | |
| Receive SCA-V final report | 32 working days | Per NETCOM Assessment & Authorization (A&A) TTP timeline |
| eMASS package approval / Receive ATO | ~45 days | |
| Final migration | ~30-45 days | Time may vary depending on amount of required migration activities |