Navigating Cybersecurity requirements for DoD Cloud deployed Mission Applications

Cybersecurity Whitepaper

Author: Jake McKinley
Independent Security Consultant
for Bull Bear Defense Solutions

CHALLENGE – MEETING ACQUISITION COST, SCHEDULE AND PERFORMANCE MILESTONES WHILE NAVIGATING CLOUD CYBERSECURITY REQUIREMENTS IN DOD

Deploying a DoD Information Technology capability to a user community in the field is always a challenge for clients to navigate due to the complexity of Information Technology capabilities, Cybersecurity requirements and customer responsibilities. This challenge can adversely affect cost, schedule and performance for programs in the DoD IT ecosystem if not carefully managed by knowledgeable and experienced staff members throughout the acquisition lifecycle.

This white paper discusses key concepts experienced by our security consultants and provides lessons learned in deploying IT capability to the user community.

OVERVIEW

The following key concepts are explained in this whitepaper and should be considered by DoD customers deploying IT capability to the Cloud.

CLOUD MODEL – IaaS/PaaS/SaaS choose wisely based on mission, budget and capability
DOD PA IMPACT LEVEL – IL2/IL4/IL5/IL6 driven by data sensitivity processed by system
HOSTING ENVIRONMENT – Cloud Provider Azure, AWS or other DoD PA approved provider
POLICY – Inch deep and mile wide, experience, tailored approach
STAFF – Qualified, experienced, knowledgeable, early engagement in acquisition as possible

CLOUD MODEL

The cloud model pursued by the customer is one of the most critical items to consider for cost, schedule and performance. Does the proposed vendor currently offer an Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) Cloud Service Offering (CSO) to its customers? IaaS, PaaS and SaaS directly correlate to the amount of work the team must complete to successfully deploy to the Cloud and obtain an Authorization to Operate (ATO) and successful production deployment. Most CSOs in the USAF and DoD today are PaaS CSOs with tailored custom software on top of the PaaS stack. This means that the ISSM and or Security Engineer must tailor in the additional security controls testing required to ensure the Confidentiality, Integrity and Availability requirements of the mission are met. The model below from the Cloud SRG demonstrates the notional division of inheritance and risk for a Cloud Service correlated to the amount of responsibility a cloud provider and ISSM/ISSO should expect.

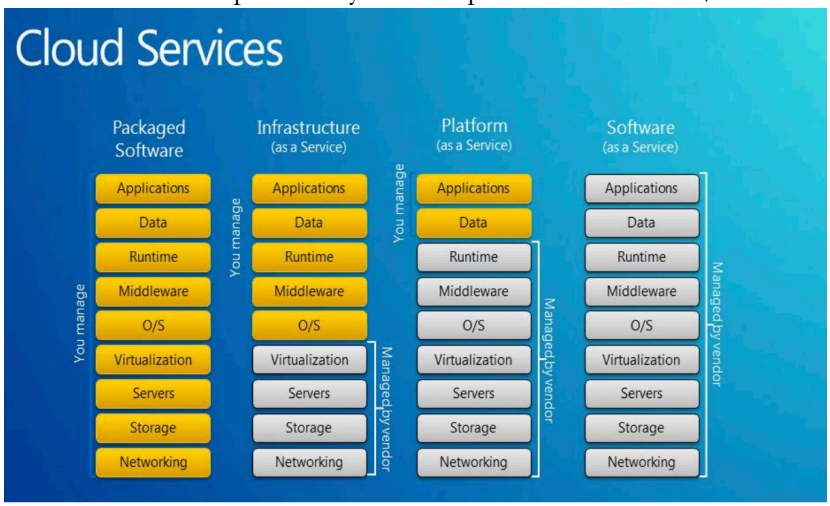

Figure 2 – Notional Division of Security Inheritance and Risk [40]
https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf

DoD PA IMPACT LEVEL

Typically, the mission owner should know what type of data their system will process. Sometimes this is not the case and the ISSM must work with and lead the Information Owner and PMO in completing the system categorization checklist (RMF step 1). This includes analyzing NIST 800-60 for the types of data that will be processed by the system and documenting these data types. The majority of IT systems in the DoD today process IL4 data on the Unclassified side of the house, however the uniqueness of the mission requirements must be considered during this process. The chart below outlines the unique requirements by Impact level mandated by the DoD.

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf

HOSTING ENVIRONMENT

Another key decision a Mission Application must make is the hosting environment in which they will deploy to. This decision should be considered with the assistance of a knowledgeable Cloud Architect if considering an Azure or AWS custom PaaS solution. If the customer is looking for a turnkey solution with considerably less security testing, consider an FedRAMP and DoD PA approved SaaS offering. However, a SaaS still has certain DoD and Mission Application considerations that must be made around Access Management, Role Based Access Control, PKI configuration, network routing through approved Cloud Access Points and additional mission specific requirements. It is worth taking the extra time to analyze the hosting environment in which the application will reside as its home. Most of the deployments today are hosted in either Azure or AWS. However, there are other Cloud Offerings on the market that meet the DoD PA IL 2-6 requirements. For more information, visit the DISA Cloud Connection site for a listing of approved CSOs. It is recommended to ensure your Cybersecurity staff are knowledgeable of the Enterprise Cloud offerings, their eMASS inheritance model and what the Cybersecurity staff will be responsible to test and maintain as part of their Mission Application ATO.

POLICY

Applicable policy depends on the strategy to deploy the Mission Application and capability to the appropriate Cloud. Policy is something that is deeply engrained in Cybersecurity. Having a knowledgeable ISSM and ISSO is paramount to executing a successful Cloud Cybersecurity program. A tailored approach to pursuing a risk determination and decision from the Mission Application is recommended. The Cybersecurity team must be proficient and knowledgeable in the following policies:

-NIST 800-53 rev 4 and 5
-NIST 800-60 vol2
-NIST 800-37
-DoD Cloud Connection Process Guide (CCPG)
-If A4 –HAF A4 A&A guide
-DISA STIGS

-DoD Cloud Security Requirements Guide (SRG) -EPL / APL processes to get approval

STAFF

One of the most valuable lessons learned in our experience is to ensure your ISSM is actively engaged to spearhead, drive the Cybersecurity milestones and engage early and often with the Program Management Office (PMO) team and Authorizing Official Designated Representatives (AODR) and Security Controls Assessor Representatives (SCAR). This active engagement will ensure clear lines of communications are kept and the necessary Government leadership are able to engage when needed to meet ensure programmatic milestones are met. The AODR and SCAR engagement are key to establishing an execution plan to deliver to cost, schedule and performance.

Cybersecurity staff should be well versed in the key differences between traditional IT policy and Cloud policy. Additionally, the Cyber team should be prepared for IT cultural challenges when standing up new IT systems in the Cloud and or migrating existing IT systems. IT cultural changes are unique and can root from older sometimes antiquated IT systems that may take significant re-engineering costs to migrate to the Cloud successfully that the mission partner may not be able to afford or staff. Finding the staff that have the experience to guide the Mission Application from start to finish can be a challenge. Cybersecurity is one of those fields that is an inch deep and a mile wide. As such, there are a wide variation of skillsets of Cybersecurity professionals that can execute and deliver an Authorization to Operate (ATO) for an IT Mission Application hosted in the Cloud. It is key to ensure your Cybersecurity staff not only know the policy, but truly understand the lift it takes to deploy to the cloud and obtain an ATO.

The ISSM should be consulting on the team as early as possible in the acquisition of the Cloud vendor, Cloud Service Provider and Integrator. This active engagement ensures the appropriate vendor and integrator communicates their required certification up prior to and after contract award. Additionally, a knowledgeable ISSM should be intimately familiar with the processes in the DoD Cloud SRG, Cloud Connection Process Guide and be able to explain these concepts to non-technical staff members. This will include the applicable DFARS and FAR clauses that will be needed in the vendor contract.

CONCLUSION

The journey to the Cloud can be a bumpy road if the customer does not account for the unique challenges outlined in this whitepaper. If you are migrating to the Cloud or a new system, consider the following outlined above to ensure your cost, schedule and performance milestones are met:

CLOUD MODEL – IaaS/PaaS/SaaS choose wisely based on mission, budget and capability
DOD PA IMPACT LEVEL – IL2/IL4/IL5/IL6 driven by data sensitivity processed by system
HOSTING ENVIRONMENT – Cloud Provider Azure, AWS or other DoD PA approved provider
POLICY – Inch deep and mile wide, experience, tailored approach
STAFF – Qualified, experienced, knowledgeable, early engagement in acquisition as possible

We look forward to serving your Cybersecurity and IT needs and navigating these challenges for your team. Please send questions about this whitepaper to:

Jessica McKinley – President Bull Bear Defense Solutions LLC
bullbeardefense@gmail.com
www.bullbeardefense.com