Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud

Ensures that the cloud service provider:
- Use government-related data only to manage the operational environment that supports the Government data and for no other purpose
- Complies with requirements for cyber incident reporting and damage assessment

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, applies when a contractor intends to use an external cloud service provider to store, process, or transmit covered defense information in the performance of a contract. DFARS Clause 252.204-7012 requires the cloud service provider to meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
DISA Cloud Computing SRG

Cloud Computing Security Requirements Guide

1 Introduction
2 BACKGROUND
3 INFORMATION SECURITY OBJECTIVES / IMPACT LEVELS
4 RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS
5 SECURITY REQUIREMENTS
6 CYBERSPACE DEFENSE AND INCIDENT RESPONSE

Appendix A - References
Appendix B - Glossary
Appendix C - Roles and Responsibilities
Appendix D - CSP Assessment Parameter Values for PA
Appendix E - Privacy Overlay Comparative C/CE Tables and Value Tables
Appendix F - FUTURE Privacy Overlay Guidance

Department of Defense
Cloud Computing Security Requirements Guide

Version 1 Release 3 | 6 March 2017

Developed by the Defense Information Systems Agency for the Department of Defense
## Impact Level = DISA-Approved Clouds

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>Information Sensitivity</th>
<th>Security Controls</th>
<th>Location</th>
<th>Off-Premises Connectivity</th>
<th>Separation</th>
<th>Personnel Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Public or Non-Critical Mission Information</td>
<td>FedRAMP v2 Moderate</td>
<td>US/US outlying areas or DoD on-premises</td>
<td>Internet</td>
<td>Virtual / Logical PUBLIC COMMUNITY</td>
<td>National Agency Check and Inquiries (NACI)</td>
</tr>
<tr>
<td>4</td>
<td>CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems</td>
<td>Level 2 + CUI-Specific Tailored Set</td>
<td>US/US outlying areas or DoD on-premises</td>
<td>NIPRNet via CAP</td>
<td>Virtual / Logical Limited “Public” Community Strong Virtual Separation Between Tenant Systems &amp; Information</td>
<td>US Persons ADP-1 Single Scope Background Investigation (SSBI)</td>
</tr>
<tr>
<td>6</td>
<td>Classified SECRET National Security Systems</td>
<td>Level 5 + Classified Overlay</td>
<td>US/US outlying areas or DoD on-premises</td>
<td>SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval</td>
<td>Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems &amp; Information</td>
<td>US Citizens w/ Favorably Adjudicated SSBI &amp; SECRET Clearance NDA</td>
</tr>
</tbody>
</table>
Cloud Computing as-a-service

SaaS
Software-as-a-service, also known as cloud application services, is the most comprehensive form of cloud computing services, delivering an entire application that is managed by a provider, via a web browser.

Software updates, bug fixes, and general software maintenance are handled by the provider and the user connects to the app via a dashboard or API. There’s no installation of the software on individual machines and group access to the program is smoother and more reliable.

You’re already familiar with a form of SaaS if you have an email account with a web-based service like Outlook or Gmail, for example, as you can log into your account and get your email from any computer, anywhere.
Fed RAMP Certification for Cloud Service Providers

www.fedramp.gov > marketplace

ATO and Assess-Only/ATU

Do I need an ATO?

Maybe not...

If the Program is proposing an internal or external IS service, such as a web-based application or SaaS, the AO will decide

IT below the system level (Single Purpose IT Products or Devices, PIT Subsystems, PIT Products, IT Products, and IT Services) or if the IS in an internal or external IS service, the AO has discretion to simply approve for use.

DEFENDED
401 K
ATTACKS BLOCKED
LAST 30D

SOI Injection
10,253
Cross-site Scripting
132,420
HTTP Anomaly
2,371
Command Injection
96,386
PHP Injection
5,522
Remote File Inclusion
62,179

DEPLOYED
23,086
Deployment Artifacts

STORAGE

DEPLOYED
17,293,670
MONTHLY LOGINS

DELIVERED
3,624 TB
TOTAL DATA STORED/HOSTED

2122 TB
Azure

1502 TB
AWS

REQUESTS BY STATE

Optimized
HITS PER SECOND (PEAK)
1,423

AVG. WEEKLY THROUGHPUT
9,176 GB

DATA OFFLOADED
60%
Advantages of Cloud One

• Cloud One is a multi-hybrid cloud environment with centrally-funded hosting that utilizes both Amazon Web Services and Microsoft Azure to host the Air Force’s enterprise general purpose applications at the Impact Levels (IL) 2, 4 and 5. As of May 2021, Additionally, Cloud One is able to support IL2 workloads in Google Cloud Platform (GCP) and will soon host higher levels of classification in both GCP and Oracle cloud offerings. When you are ready to begin or continue your cloud journey, the Cloud One team will discuss your capability needs and provide a way forward with an approved delivery partner.

• Cloud One provides a plethora of services that will accelerate the accreditation process, ensure continuing compliance with security controls, and facilitate rapid future deployment of capabilities. We need to take advantage of the rapid ATO-inheritance and Real-time Compliance that Cloud One offers. Additionally, Cloud One offers a wide range of native cloud services, including DISA-approved “guardrails” that allow system and application owners to focus on maintaining their applications rather than spending valuable time managing their own hosting environment and underlying infrastructure.
DevSecOps/Platform One/Cloud One Relationship

Continuous Monitoring
Leverages the Sidecar Container Security Stack

Development Teams can build software/microservices leveraging hardened containers

Brings baked-in security and Microservices architecture enablement

Fully containerized, leverages DoD approved containers from DCAR Development Team selects tools from approved K8S stacks

CNCF compliant Kubernetes (K8S)
Includes Site Reliability Engineers (SREs) etc.
Development Team selects between approved K8S stacks

Environment Agnostic
Cloud One Preferred for unclassified (IL2, IL4, IL5)
Or SC2S/C2S/FENCES
Or on-premise/classified environments

Application Layer
Service Mesh Layer
Continuous Integration / Continuous Delivery (CI/CD) Layer
Platform Layer
Infrastructure Layer

YOU
PLATFORM ONE
CLOUD ONE

milCloud® 2.0
Capabilities
### milCloud® 2.0 Benefits

<table>
<thead>
<tr>
<th>Secure</th>
<th>Easy to Use</th>
<th>Affordable</th>
</tr>
</thead>
</table>
| Dozens of inherited critical security controls not available in commercial clouds, including:  
- DoD Information Network Security Boundary Controls  
- DISA Data Center Physical Facility Security Controls DECCS  
- GDIT’s FedRAMP High Accreditation & Controls  
- DISA’s IL-5 Provisional Authority Accreditation & Controls (IL-6 coming soon)  
- Virtual Trusted Platform Manager (vTPM) provided through VMWare, providing encrypted virtual machines and storage | Customers can buy cloud services in as few as 48 hours, compared to typical months-long acquisition processes  
- Self-service model for service ordering, service provisioning, and account management and funding  
- Customers can use MIPR funds or a credit card to buy any services on contract (all FFP)  
- Funds are fungible: infrastructure hosting, engineering & migration services, and consulting & professional services  
- Funds can cross fiscal years depending on color of money | Compute, storage, and network cloud services priced at commercial parity – with enhanced security  
- “Pay-as-you-go” model – customers only pay for what they use  
- No à la carte bandwidth or transaction fees charged to access applications or data  
- FFP Services enable predictable spend patterns and transparent cost understanding  
- One-stop shop for hosting, engineering, consulting, and professional services |

milCloud® 2.0 is held by CSRA, LLC, a General Dynamics Information Technology (GDIT) managed affiliate. milCloud® and the milCloud® logo are registered trademarks owned by the Defense Information Systems Agency (DISA).
Cloud Threat Landscape
www.dc3.mil
>>DIB Cybersecurity
>>DCISE Analytics
References

- Cloud One: https://cloudone.af.mil/
- Platform One: https://p1.dso.mil/
- Mil Cloud https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/Fact-Sheet-milCloud-2-0.ashx

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: [https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/](https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/)
- Please provide questions, feedback or if you just want to talk about your cyber security/data protection questions at [https://www.safcn.af.mil/Contact-Us/](https://www.safcn.af.mil/Contact-Us/)
  - Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!
  - **Every Tuesday**, 1pm Eastern, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything.