Risk Management in the Cloud

RMF Strategies for Cloud-based Systems and Architectures

Alan Hardman

Defense Health Agency, *Chief Risk Management Executive Division*

UNCLASSIFIED

Agenda

1 Cloud Service Types

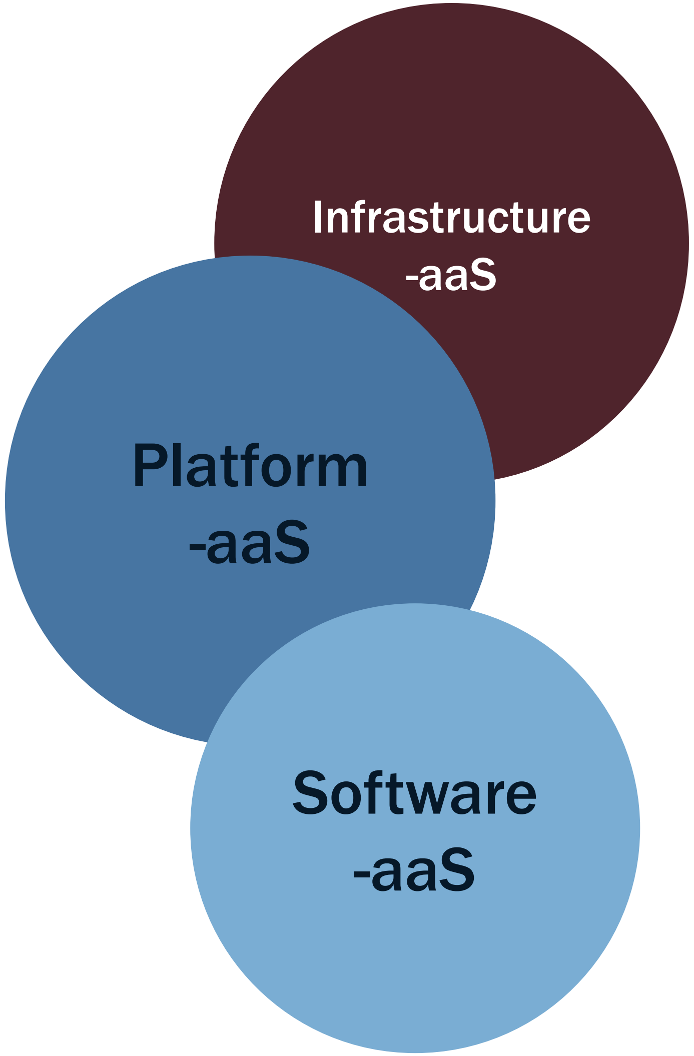
2 Federal, DOD, and DHA Requirements for the Cloud

3 Getting to the Cloud

4 Recap: Successful Programs Do…

Service Types

NIST recognizes several formal service models



IaaS

CSP manages hardware and virtualization

PaaS

Vendor additionally manages OS and related tech

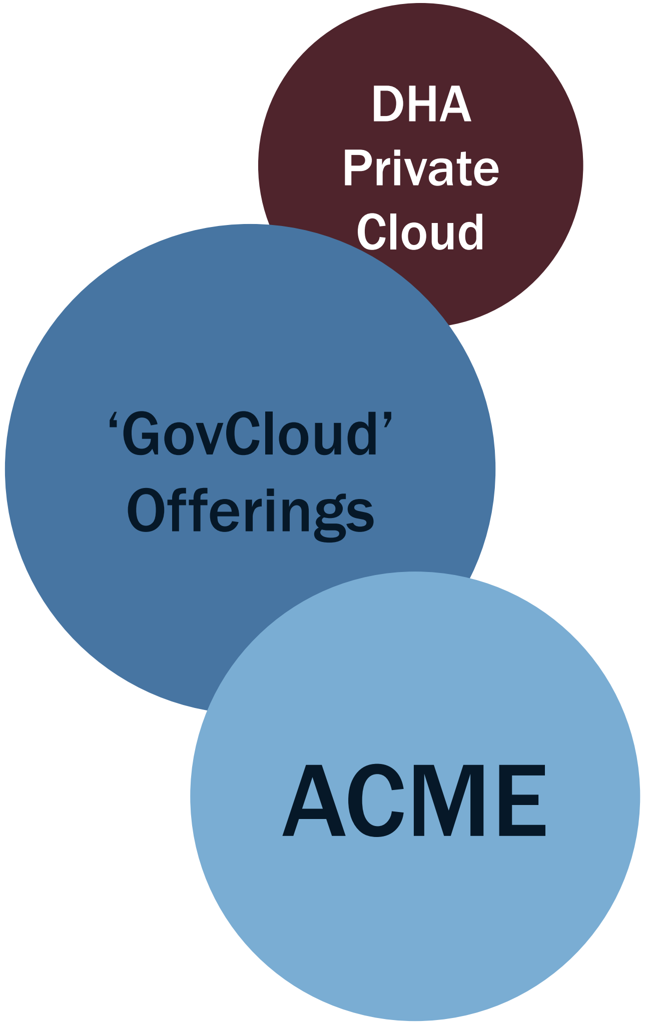
SaaS

CSP manages the full tech stack, from hardware to software

UNCLASSIFIED

Deployment Models

NIST recognizes several formal deployment models



Private

CSOs dedicated to single customer – down to the hardware

Community

Multi-tenant cloud for the exclusive use of a specific group of organizations

Public

CSOs open for use by anyone

What Are My Options?

Fully External CSO

- Vendor Provided CSOs (SaaS, PaaS, IaaS)
- Other Gov Hosted

Virtually On-Prem (MedCOI)

- DHA-managed Azure / AWS
- DHA Private Cloud (CSMS, MAAG, Local)
- DSOCC

Fully External Non-CSO

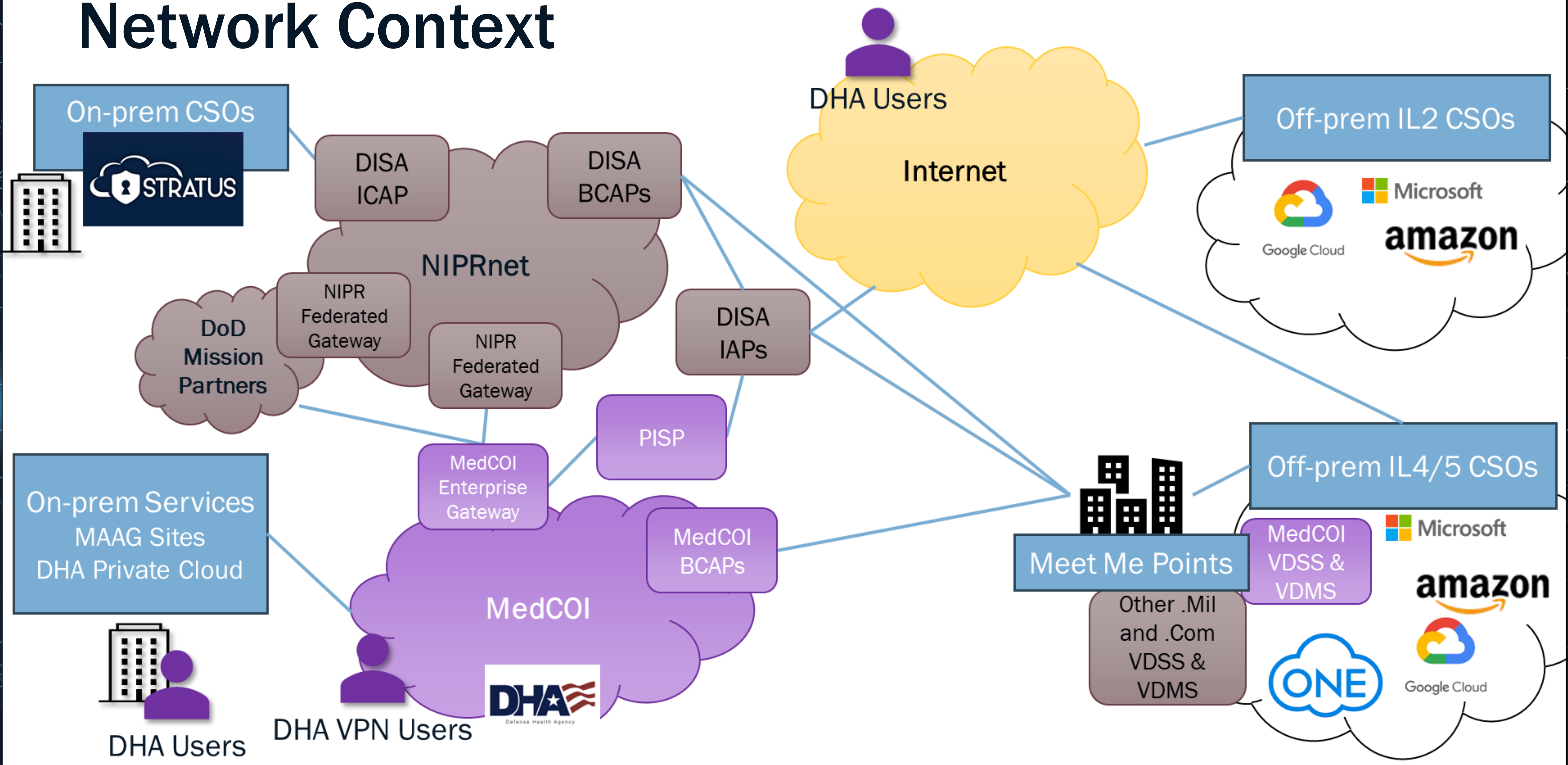
- Traditional External IT
- Non-DOD IT

For all Cloud and hosting requirements submit a request to CBS: https://hosting.health.mil

See the ESA-BAD Cloud Broker Service page for details: https://info.health.mil/dadio/ESABAD/ESABAD-SAB/CBS/Pages/CBSHome.aspx

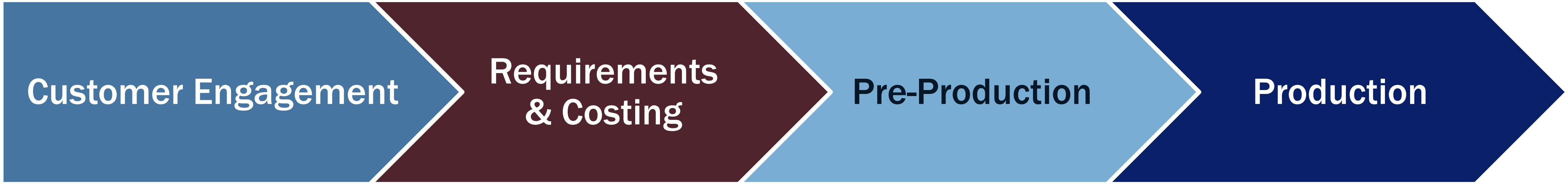
UNCLASSIFIED

Network Context



How Do I Get To The Cloud?

ESA-BAD Cloud Broker Service Hosting Process



Customer Engagement

Requirements & Costing

Pre-Production

Production

- Portal Request
- Consultative Review
- **RMED Cyber Strategy**

- Architecture Review
- Accept Design
- ESA-BAD Cost Estimate & Funding
- **RMED Cost Estimate & Funding**

- Configure and test environment
- **Execute RMF process**

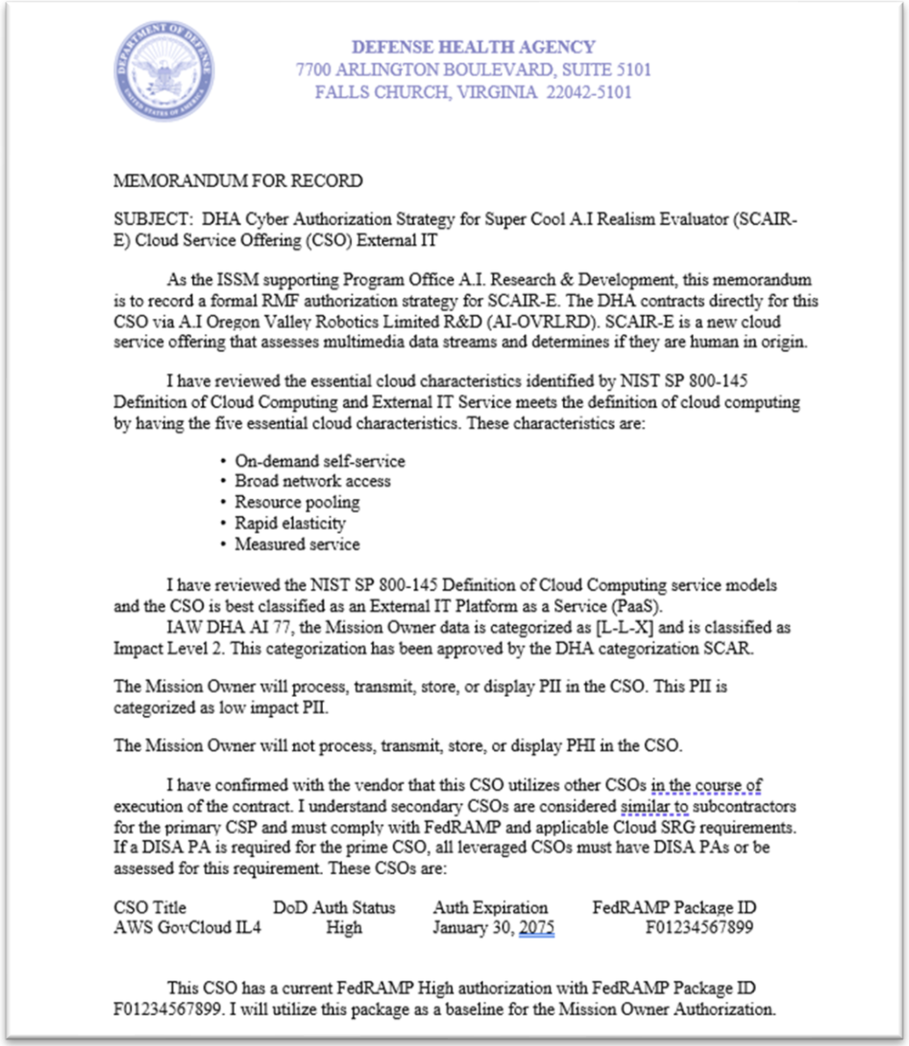
- Validate deployment
- Go-live
- **Monitor and maintain**

Cyber Strategy

Customer Engagement
Requirements & Costing
Pre-

- Portal Request
- Consultative Review
- RMED Cyber Strategy

- Assists RMF stakeholders navigating the DoD RMF requirements for cloud systems,
- Data Categorization, guided questionnaire, memorandum, supporting documents
- NOT REQUIRED FOR ON-PREM



DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

MEMORANDUM FOR RECORD

SUBJECT: DHA Cyber Authorization Strategy for Super Cool A.I Realism Evaluator (SCAIR-E) Cloud Service Offering (CSO) External IT

As the ISSM supporting Program Office A.I. Research & Development, this memorandum is to record a formal RMF authorization strategy for SCAIR-E. The DHA contracts directly for this CSO via A.I Oregon Valley Robotics Limited R&D (AI-OVRLRD). SCAIR-E is a new cloud service offering that assesses multimedia data streams and determines if they are human in origin.

I have reviewed the essential cloud characteristics identified by NIST SP 800-145 Definition of Cloud Computing and External IT Service meets the definition of cloud computing by having the five essential cloud characteristics. These characteristics are:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

I have reviewed the NIST SP 800-145 Definition of Cloud Computing service models and the CSO is best classified as an External IT Platform as a Service (PaaS).

IAW DHA AI 77, the Mission Owner data is categorized as [L-L-X] and is classified as Impact Level 2. This categorization has been approved by the DHA categorization SCAR.

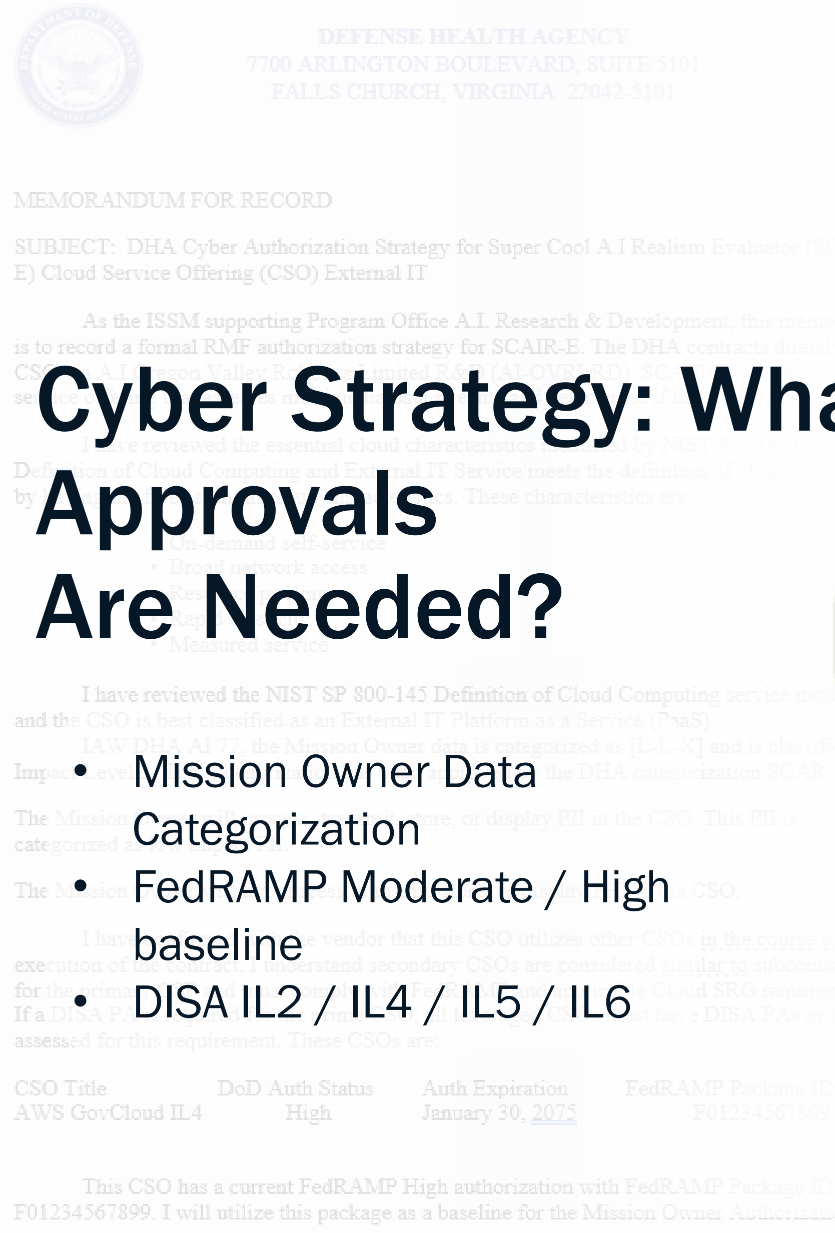
The Mission Owner will process, transmit, store, or display PII in the CSO. This PII is categorized as low impact PII.

The Mission Owner will not process, transmit, store, or display PHI in the CSO.

I have confirmed with the vendor that this CSO utilizes other CSOs in the course of execution of the contract. I understand secondary CSOs are considered similar to subcontractors for the primary CSP and must comply with FedRAMP and applicable Cloud SRG requirements. If a DISA PA is required for the prime CSO, all leveraged CSOs must have DISA PAs or be assessed for this requirement. These CSOs are:

CSO Title	DoD Auth Status	Auth Expiration	FedRAMP Package ID
AWS GovCloud IL4	High	January 30, 2075	F01234567899

This CSO has a current FedRAMP High authorization with FedRAMP Package ID F01234567899. I will utilize this package as a baseline for the Mission Owner Authorization.



DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

MEMORANDUM FOR RECORD

SUBJECT: DHA Cyber Authorization Strategy for Super Cool A.I Realism Evaluator (SCAIR-E) Cloud Service Offering (CSO) External IT

As the ISSM supporting Program Office A.I. Research & Development, this memorandum is to record a formal RMF authorization strategy for SCAIR-E. The DHA contracts directly for the CSO [illegible] A.I Oregon Valley Robotics Limited R&D (AI-OVRLRD). SCAIR-E [illegible] service [illegible]

I have reviewed the essential cloud characteristics identified by NIST SP 800-145 Definition of Cloud Computing and External IT Service meets the definition of cloud com[illegible] by [illegible] characteristics. These characteristics are:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

I have reviewed the NIST SP 800-145 Definition of Cloud Computing service mod[illegible] and the CSO is best classified as an External IT Platform as a Service (PaaS).

IAW DHA AI 77, the Mission Owner data is categorized as [L-L-X] and is classified Impact Level [illegible] the DHA categorization SCAR.

The Mission [illegible] will process, transmit, store, or display PII in the CSO. This PII is categorized as low impact PII.

The Mission [illegible] the CSO.

I have [illegible] the vendor that this CSO utilizes other CSOs in the course of execution of the contract. I understand secondary CSOs are considered similar to subcontractors for the primary CSO and must comply with FedRAMP and applicable Cloud SRG requirements. If a DISA PA is required for the prime CSO, all leveraged CSOs must have DISA PAs or be assessed for this requirement. These CSOs are:

CSO Title	DoD Auth Status	Auth Expiration	FedRAMP Package ID
AWS GovCloud IL4	High	January 30, 2075	F01234567899

This CSO has a current FedRAMP High authorization with FedRAMP Package ID F01234567899. I will utilize this package as a baseline for the Mission Owner Authorization.

Cyber Strategy: What Approvals Are Needed?

- Mission Owner Data Categorization
- FedRAMP Moderate / High baseline
- DISA IL2 / IL4 / IL5 / IL6

Defense Health Agency

DHA

- Mission Owner ATO
- J6 ESA-BAD Cloud/Hosting Governance

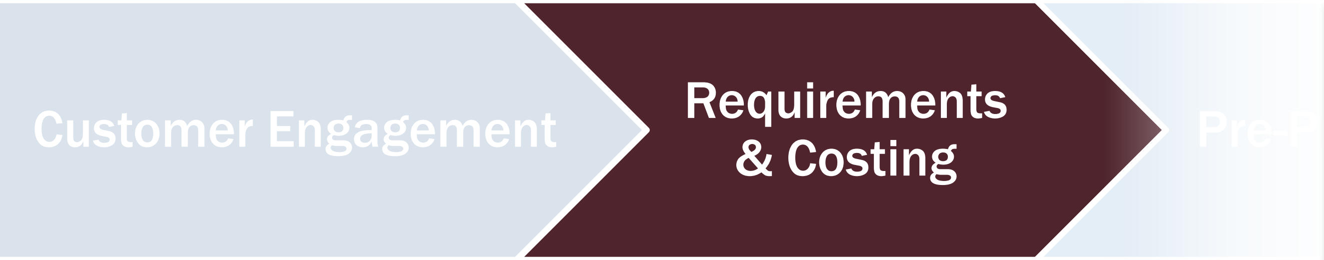
DISA

- DISA Provisional Authorization
- FedRAMP+

FedRAMP

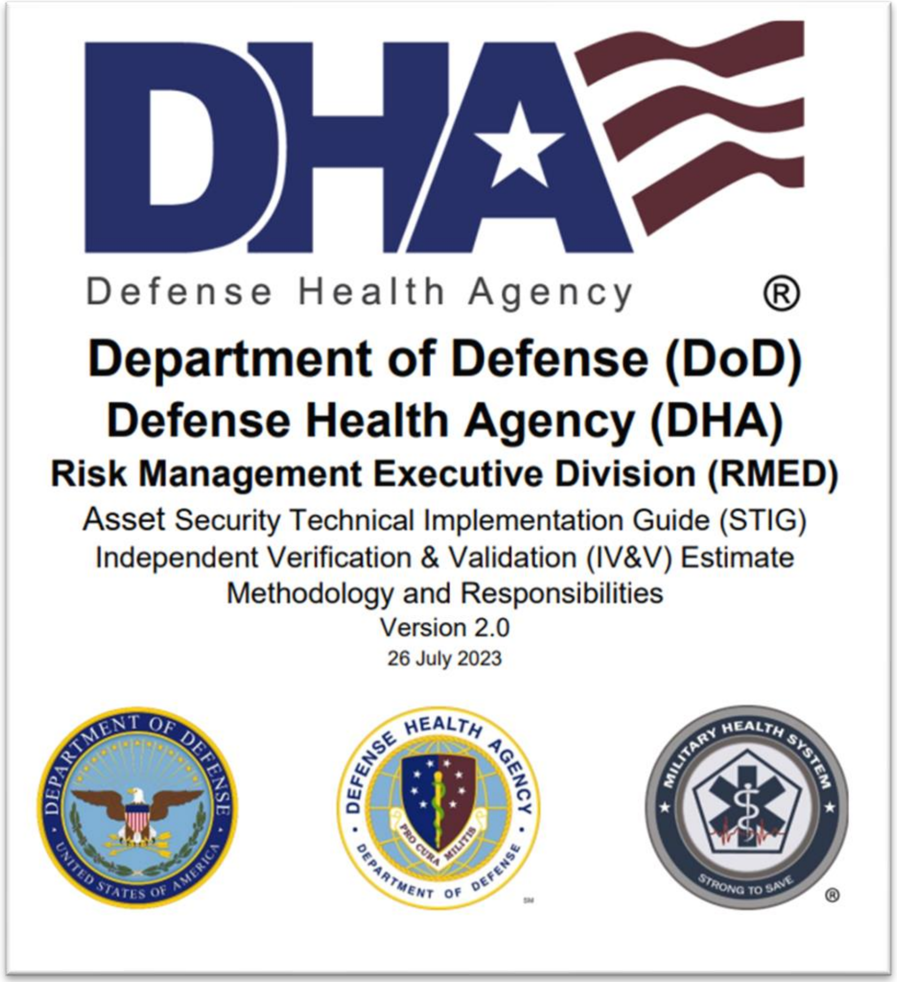
- Provisional ATO (P-ATO)
- FedRAMP Authorized (Agency ATO)

RMED Cost Estimate



- Architecture Review
- Accept Design
- ESA-BAD Cost Estimate & Funding
- RMED Cost Estimate & Funding

- Standard RMED Cost Estimate Process
- Guided by Cloud Authorization Strategy


DHA

Defense Health Agency ®

Department of Defense (DoD)

Defense Health Agency (DHA)

Risk Management Executive Division (RMED)

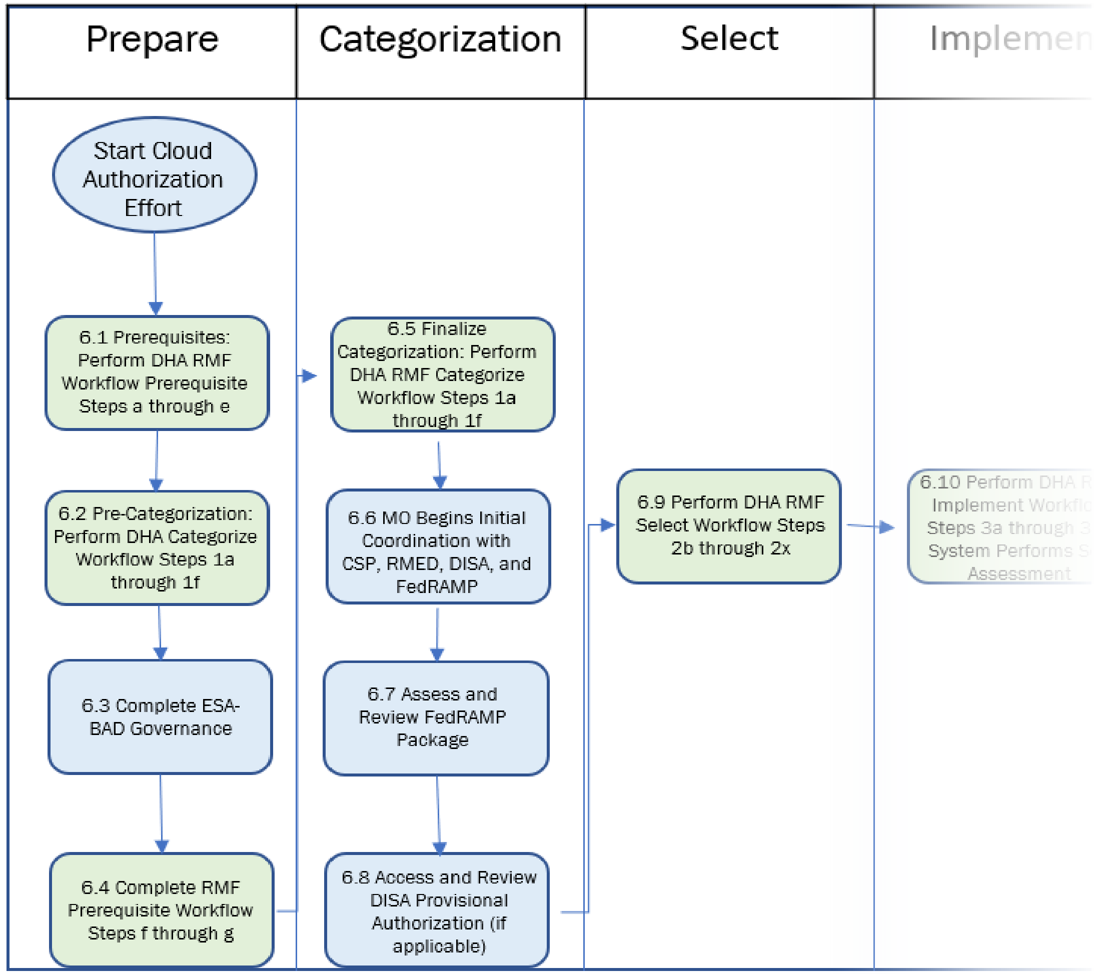
Asset Security Technical Implementation Guide (STIG)
Independent Verification & Validation (IV&V) Estimate
Methodology and Responsibilities

Version 2.0

26 July 2023

UNCLASSIFIED

Execute RMF



Prepare

Categorization

Select

Implemen

Start Cloud Authorization Effort

6.1 Prerequisites: Perform DHA RMF Workflow Prerequisite Steps a through e

6.2 Pre-Categorization: Perform DHA Categorize Workflow Steps 1a through 1f

6.3 Complete ESA-BAD Governance

6.4 Complete RMF Prerequisite Workflow Steps f through g

6.5 Finalize Categorization: Perform DHA RMF Categorize Workflow Steps 1a through 1f

6.6 MO Begins Initial Coordination with CSP, RMED, DISA, and FedRAMP

6.7 Assess and Review FedRAMP Package

6.8 Access and Review DISA Provisional Authorization (if applicable)

6.9 Perform DHA RMF Select Workflow Steps 2b through 2x

6.10 Perform DHA R Implement Workflo Steps 3a through 3 System Performs S Assessment

Pre-Production

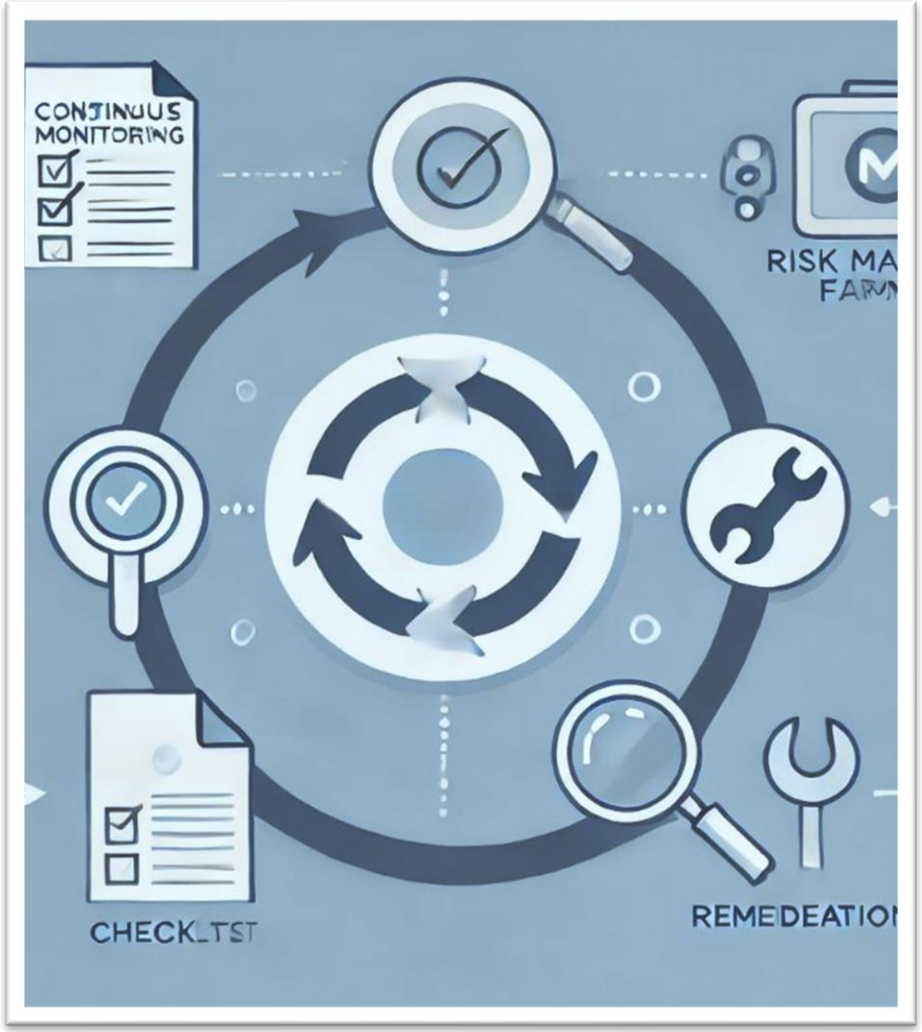
Production

- Configure and test environment
- Execute RMF Process

- Achieve Authorization
  - CNS SOPs & CSO configurations
  - STIGs, SRGs, novel technologies
  - SLA (service availability)
  - Interconnections
- Coordinate with DHA CSSP
- Coordinate with ESA-BAD

UNCLASSIFIED

Monitor & Maintain



Pre-Production

Production

- Validate deployment
- Go-live
- Monitor & Maintain

- Continuous Monitoring
  - RMF: DHA, FedRAMP, DISA PA
  - DHA CSSP
- Change Control Oversight
  - RMED, ESA-BAD

UNCLASSIFIED

Recap: Successful Programs…

…select CSOs postured for success

- DISA PA
- FedRAMP Moderate/High
- Contract language & SLAs
- Understand the CSO – Shared Responsibility Model
- Know your requirements!

…plan programmatics & funding

- Staffing for DHA ISSM/ISSO
- RMF costs
- Staffing for CSO administration
- CSO licensing costs
- Transition costs

…stay engaged & coordinate!

- Vendor
- ESA-BAD governance & engineering
- RMED RMF
- DHA CSSP monitoring

UNCLASSIFIED

Contact:

Al Hardman
Defense Health Agency, Chief Risk Management Executive Division

alan.c.hardman.civ@health.mil