RESTON

CMMC ENCLAVES BY INDUSTRY

DANIEL AKRIDGE

2025

www.cs2.cloud/reston

DANIEL AKRIDGE

Director of Engagement, Summit 7

- Recovering IT guy of 17 Years.
- Current sales guy at S7.
- Co-Host of CUI Hotline
- Worked for MSPs & Army Material Command
- When I was 10, I was a fire safety clown for the Red Cross. Points for anyone that guesses my name.

Agenda

1. What is an Enclave
2. Should you do one?
3. Dataflow & YOU
4. Manufacturing Enclaves
5. Architectural, Engineering and Construction (AEC) Enclaves
6. Regulated Research Enclaves
7. How do I pick an enclave vendor?
8. Questions

What is an enclave?

Satisfaction of CMMC security requirements may be accomplished by people, processes, or technologies which apply to the entire OSA enterprise. This **does not** mean all assets across the entire OSA enterprise are automatically part of a CMMC Assessment Scope.

- CMMC L2 Scoping Guidance

Should you do one?

1. Do you know where all your CUI is?

2. Do more than 15% of your users need access to CUI to perform the work?

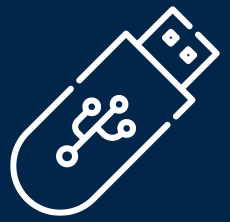
3. Can your dataflow support an enclave?

Sidenote: IT cannot answer these questions. Don’t @ me.

Dataflow & You

CNC
Machine

Printer



USB

Laptops

Mobile Devices

Servers

3rd Party Clouds

Email

Dataflow & You

M365 Content Search

Email

CUI Examples:

CUI//SP-CTI

CUI//SP-EXPT

CUI//SP-NNPI

DoD Clauses:

DoD Directive 5230.25
DoD Directive5230.25

DFARS 252.204-7012

DFARS 252.204-7048

DoD Distribution Statements:

DISTRIBUTION STATEMENT B

DISTRIBUTION STATEMENT C

DISTRIBUTION STATEMENT D

DISTRIBUTION STATEMENT E

DISTRIBUTION STATEMENT F

Ok Daniel, I can do an enclave.

Manufacturing

AEC

Regulated Research

Manufacturing

- Needs to be able to receive CUI in a compliant manner
  - File sharing and/or Email
- Needs to be able to leverage specific applications to perform the work
  - AutoCAD, SolidWorks, etc….
- Needs to be able to print drawings for assemblies
- Needs to be able to move data into the shop floor / OT Environment (*Specialized Assets*)

Manufacturing

Specialized Assets

Assets that may or may not process, store, or transmit CUI

Assets include Gov't Property, IoT, Operational Technology, Restricted Info Systems, and Test Equipment

Programmable logic controllers (PLCs)
Supervisory control and data acquisition systems (SCADA)
Distributed control systems (DCS)
Computer numerical control (CNC) systems

Requirements

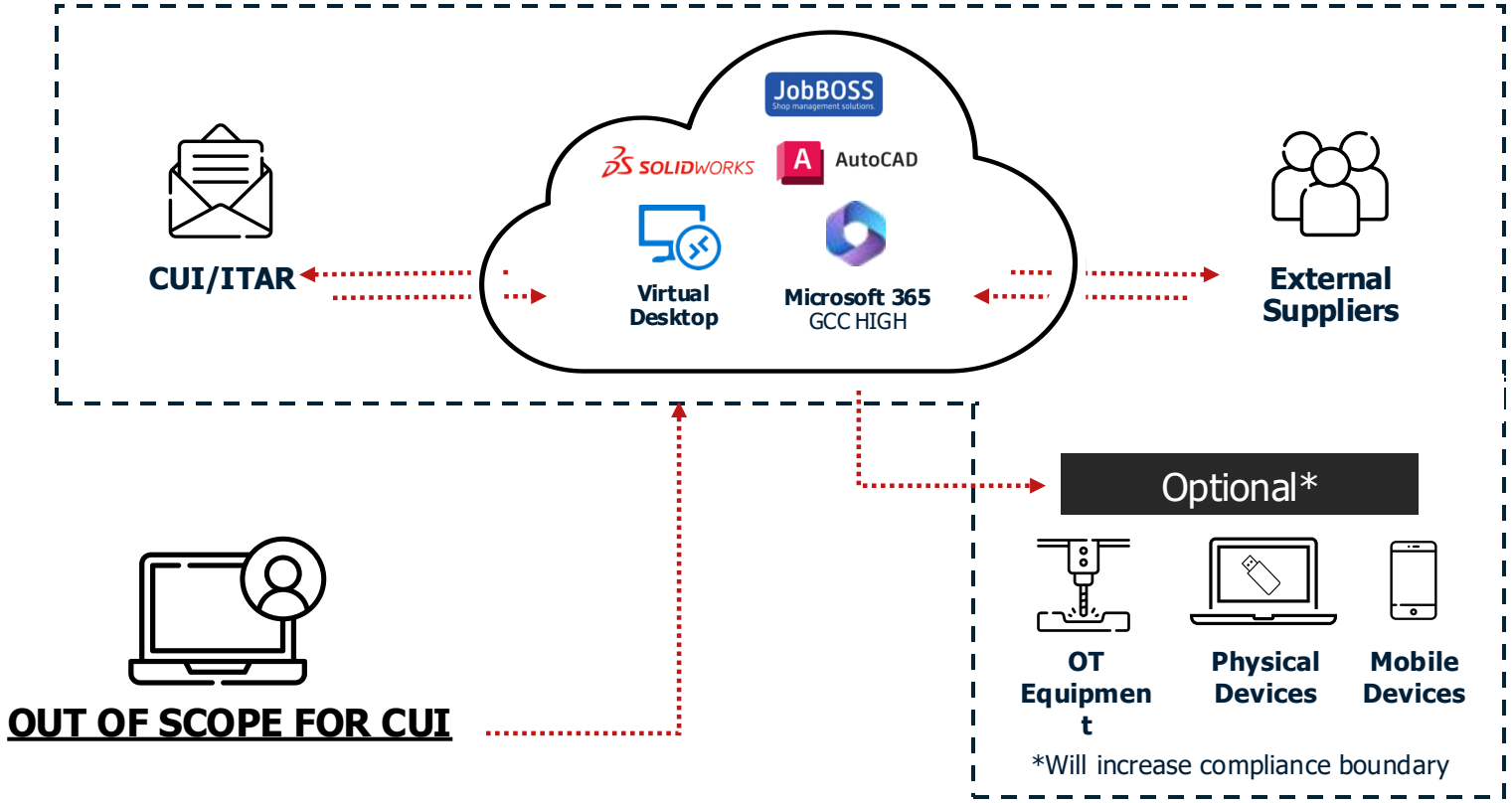
Document the SSP to show

they are managed using the **contractor's Risk based security policies, procedures, and practices**

Review the SSP in accordance with practice CA.L2-3.12.4

Do not assess against other CMMC Practices

Manufacturing



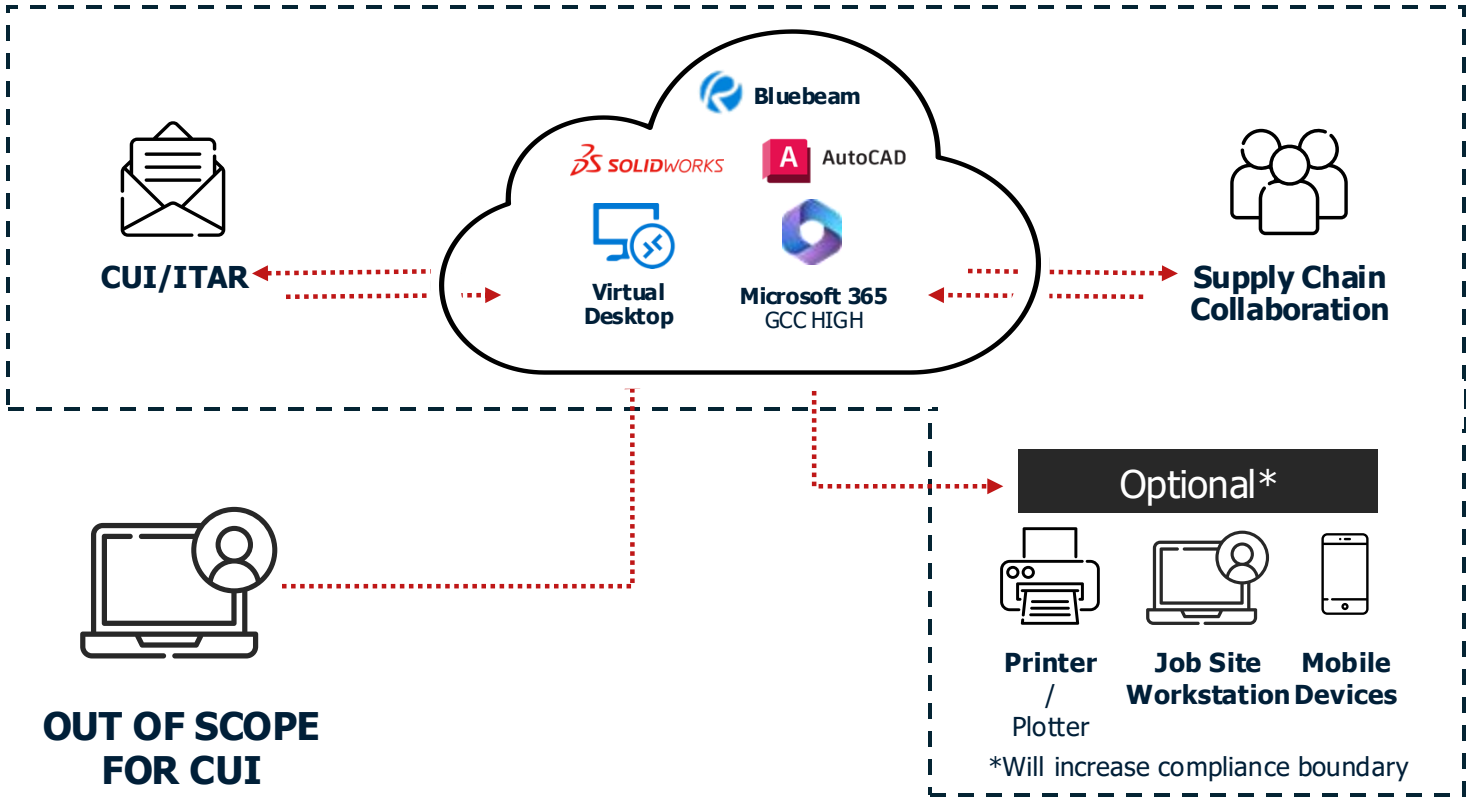
Considerations:

- If you bring On-Premises into scope, Physical Protection & Security will apply to your environment.
- Physical workstations might make more sense than all virtual desktops.
- However, print jobs are sent in plain text, consider an approved USB printer or separate network.
- Leverage FIPS 140-2 validated Encrypted USBs like Apricorn.

AEC (Architectural, Engineering, and Construction)

- Needs to be able to receive CUI in a compliant manner
  - File sharing and/or Email
- Needs to be able to leverage specific applications to perform the work
  - AutoCAD, SolidWorks, etc....
- Needs to be able to plot blueprints, schematics, etc...
- Needs tablets for jobsites to take pictures, review drawings, etc...

AEC (Architectural, Engineering, and Construction



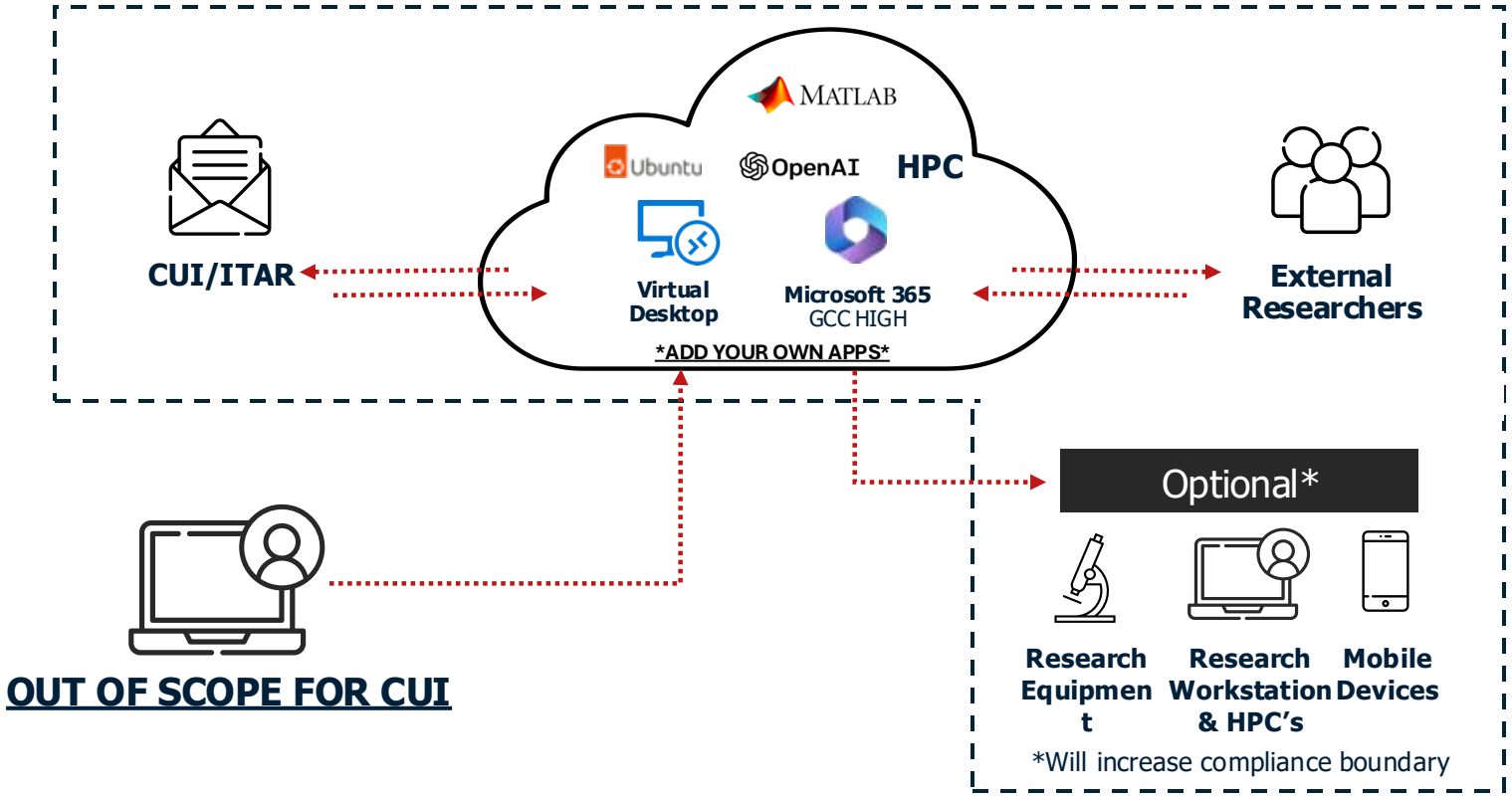
Considerations:

- Intune for iOS/Android enrollment for being able to take pictures of job sites.
- Leverage a Site-to-Site VPN connection for pooled licensing servers for expensive / critical applications.
- Secure a specific room has the “physical/print” CUI room.
- Access to the enclave for your supply chain.

Regulated Research

- Needs to be able to receive CUI in a compliant manner
  - File sharing and/or Email
- Needs to be able to leverage specific applications to perform the work
  - MatLab, Python, etc....
- Needs to be able to connect to multiple research labs
- Needs to be able to segment non-US persons away from Export Control data
- Needs to be able to carve out charge back to individual grants/contracts/research

Regulated Research



Considerations:

- Leverage Purview Site Containers and Custom Attributes for US vs. Non-US Persons in the tenant.
- Site to Site VPN for connection to labs.
- Ability to join physical devices to M365 GCCH for local CUI access.
- Ability for charge back per subscription to unique contracts/grants.

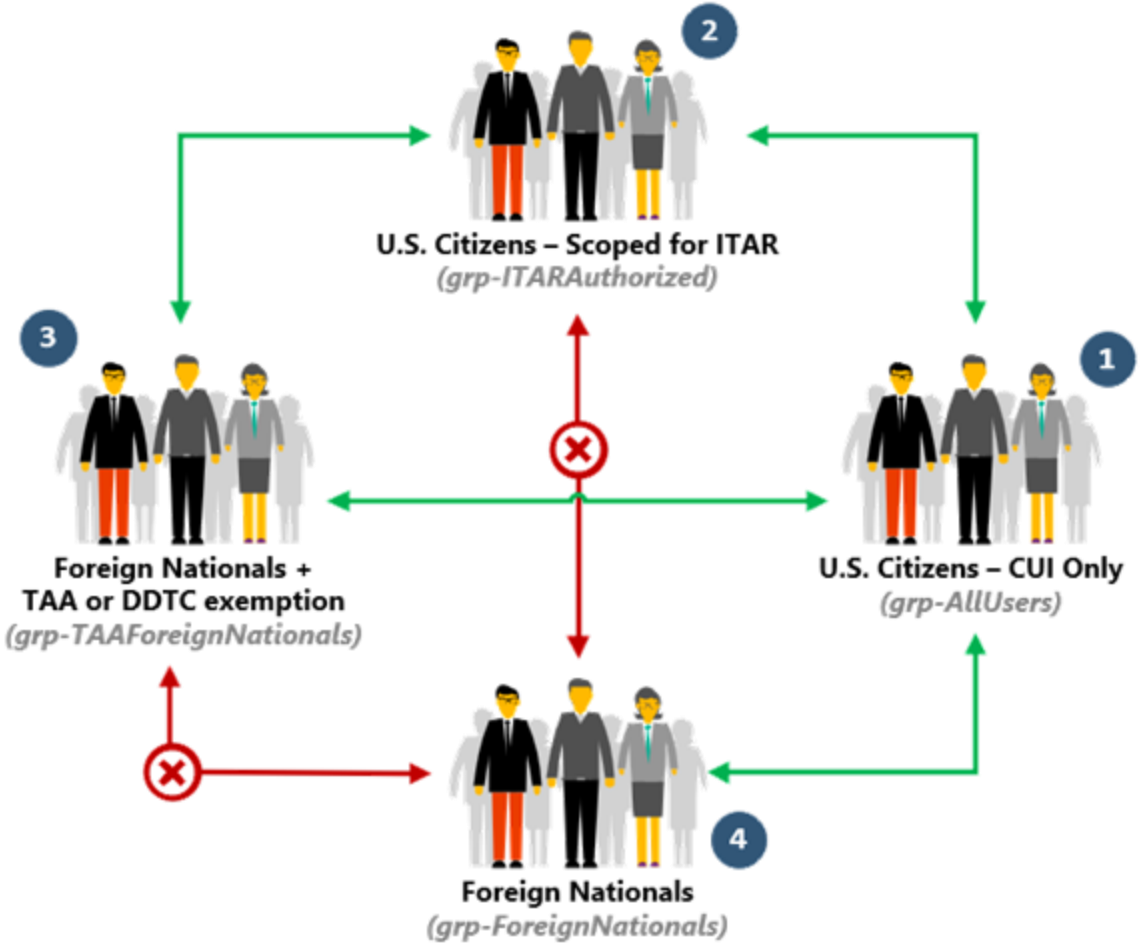
Regulated Research

What does a charge back model look like?

Azure Government (Global Monitoring) - $2,200 /Month		
Research #1	MatLab, OpenAI, MySQL, Ubuntu	$5,000 /Month
Research #2	Windows VM	$2,000 /Month
Research #3	HPC	$1,000 /Month

Regulated Research

How do you work through
non-US & US Persons in the tenant?



How do I pick an enclave vendor?

“Hosted” Enclave

- Vendor owns the hardware, hard to scale on-demand
- Vendor would need to meet FedRAMP Moderate / Equivalency
- Hard to get your data if you decide to break up
- Difficult to extend your boundary for on-premise systems
- Still needs to provide some sort of Shared/Customer Responsibility Matrix

V.S.

Managed Enclave

- You own the Microsoft 365 tenant; easy to scale on-demand
- Access to Microsoft’s FedRAMP High System Security Plan (SSP)
- You always retain access your data, even after support has ended
- Easy to extend your boundary to on-premise if needed
- Microsoft (GCCH) supports it with US Persons

Questions?

Daniel.akridge@summit7.us

linkedin.com/in/danielakridge/

Call/Text: 256.426.1232