How to Properly Scope Your Assessment

Thad Wellin, CISSP, CCP

TRW
Security Solutions

Agenda

- About Me
- How we got here
- How to start
- What is CUI
- Data flows
- Scoping
- Enclave vs Enterprise
- Enclave examples

About Me

- **Certifications\Degree**
  - Certified Information Systems Security Professional (CISSP)
  - Certified CMMC Professional (CCP)
  - Certified Expert RMF Professional (CERP)
  - Security +
  - M.S. Information Security & Assurance

- **Information Systems Security Manager/Information Assurance Engineer**
  - RMF A&A/DIACAP C & A
  - Engineer baked security into development efforts

- **Consultant, Cyber Security**
  - Governance, Risk Management and Compliance

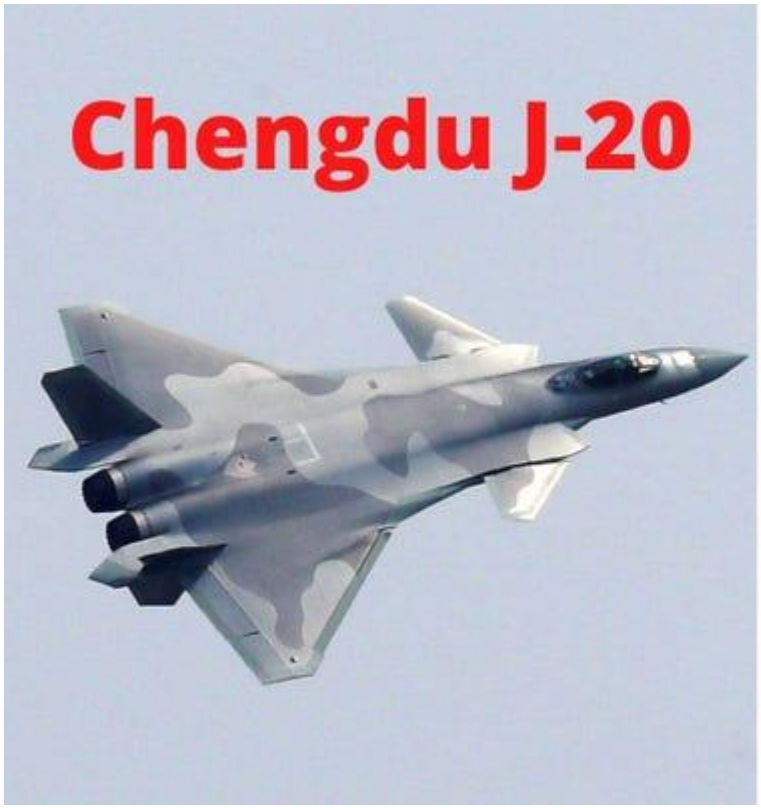
- **Retired USAF – Information Assurance**

How it started

- **All started with the 9/11 Commission**
  - Legacy CUI was labeled and handled differently from the different Federal Agencies and DoD Services
    - Example- FOUO/SBU/OUO
- **Controlled Unclassified Information was Established by Executive Order 13556 in November 2010**
- **Implemented by 32 CFR part 2002 in Sep 2016**
  - 2002.4(m) ***CUI Executive Agent (EA)*** is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

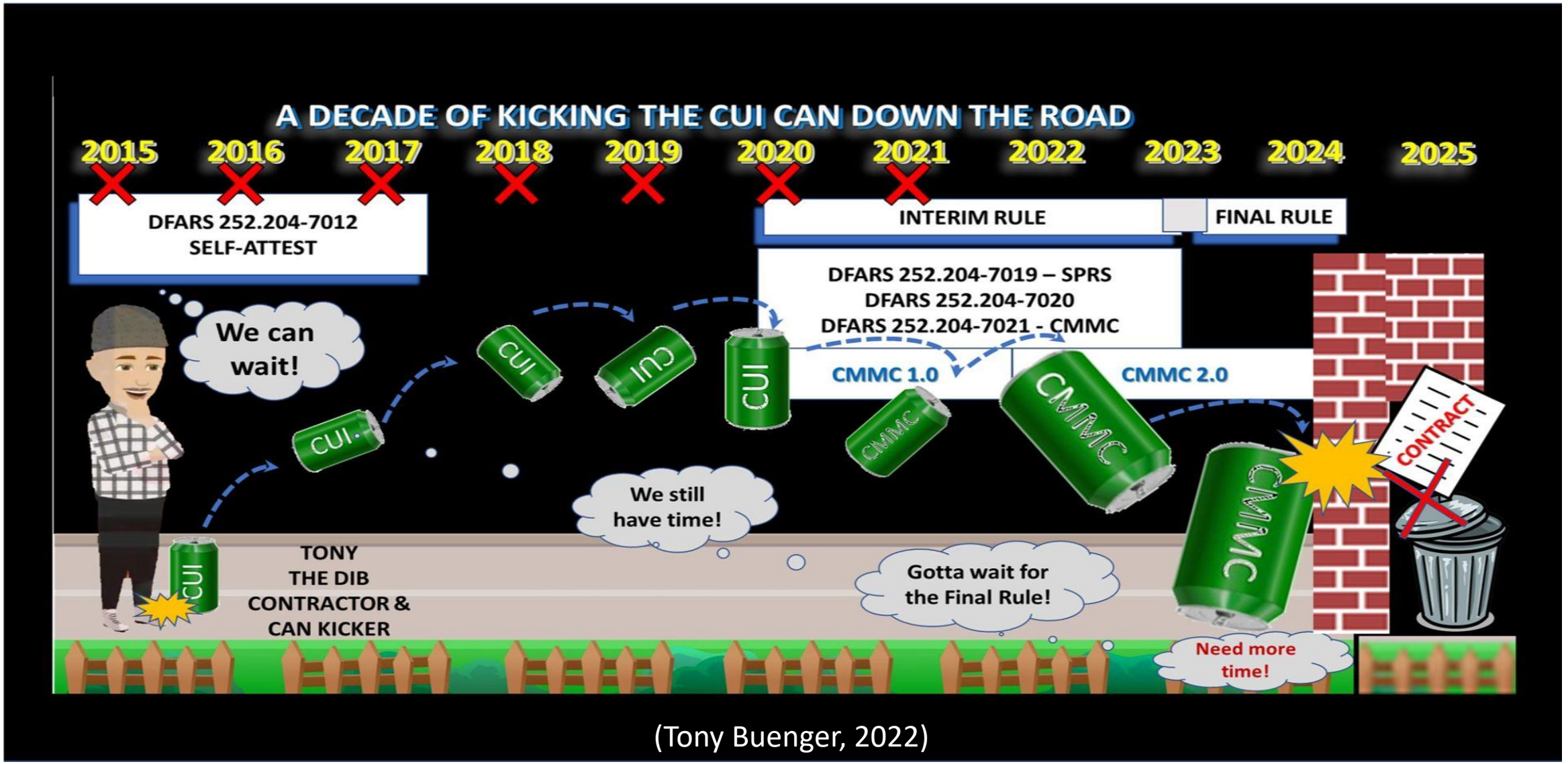
  - 2002.14(h)(2) NIST SP 800-171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

Why we need CMMC



- F-22 took 16 years to develop
- J-20 took 8 years

Can we wait any longer?



(Tony Buenger, 2022)

How to start

- Identify what data is CUI (CTI, Export Controlled)
- Understand Dataflow
  - How is the data used?
  - What devices is it used on?
  - How is it shared?
- Create Dataflow diagrams/Establish CUI Boundary
- Identify what is used to protect CUI
  - People, Processes and Technologies
- Create Detailed Asset Inventory
  - Categorize Assets
- Create the System Security Plan and apply controls
  - Draft POAMs for open controls

What is CUI

Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

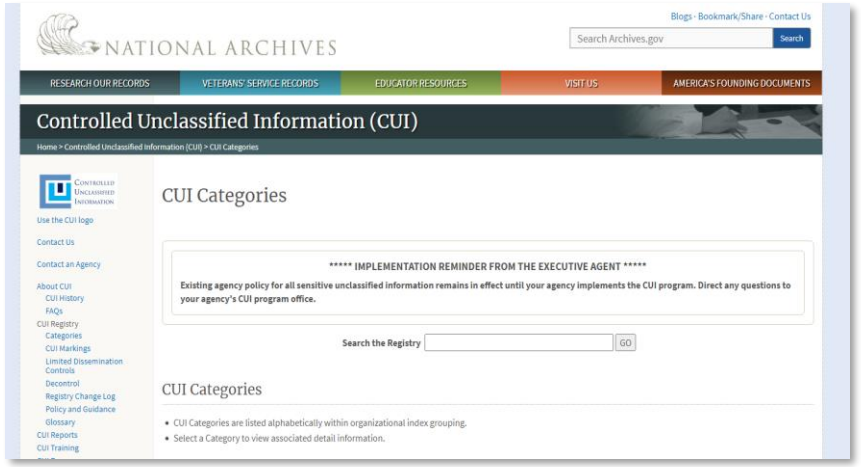
- Look for Distribution Statements B through F in CDRLs
- Is it Export Controlled (EAR or ITAR)
- Does the contract require the design specific to Military or Space or modification of COTS for Military or Space
- Ask your contracting officer for guidance

WHAT IS *NOT* CUI?

- Classified information
- Corporate intellectual property (unless created for or included in requirements related to a government contract)
- Publicly available information

What is CUI

1 [ISOO Registry](https://www.archives.gov/cui/registry/category-list) The National CUI Registry contains Indexes and categories for the entire Executive Branch and should be consulted for non-DOD contracts.



https://www.archives.gov/cui/registry/category-list

2 [DoD Registry](https://www.dodcui.mil/Home/DoD-CUI-Registry) The DOD CUI Registry aligns each Index and Category to DOD issuances.

https://www.dodcui.mil/Home/DoD-CUI-Registry

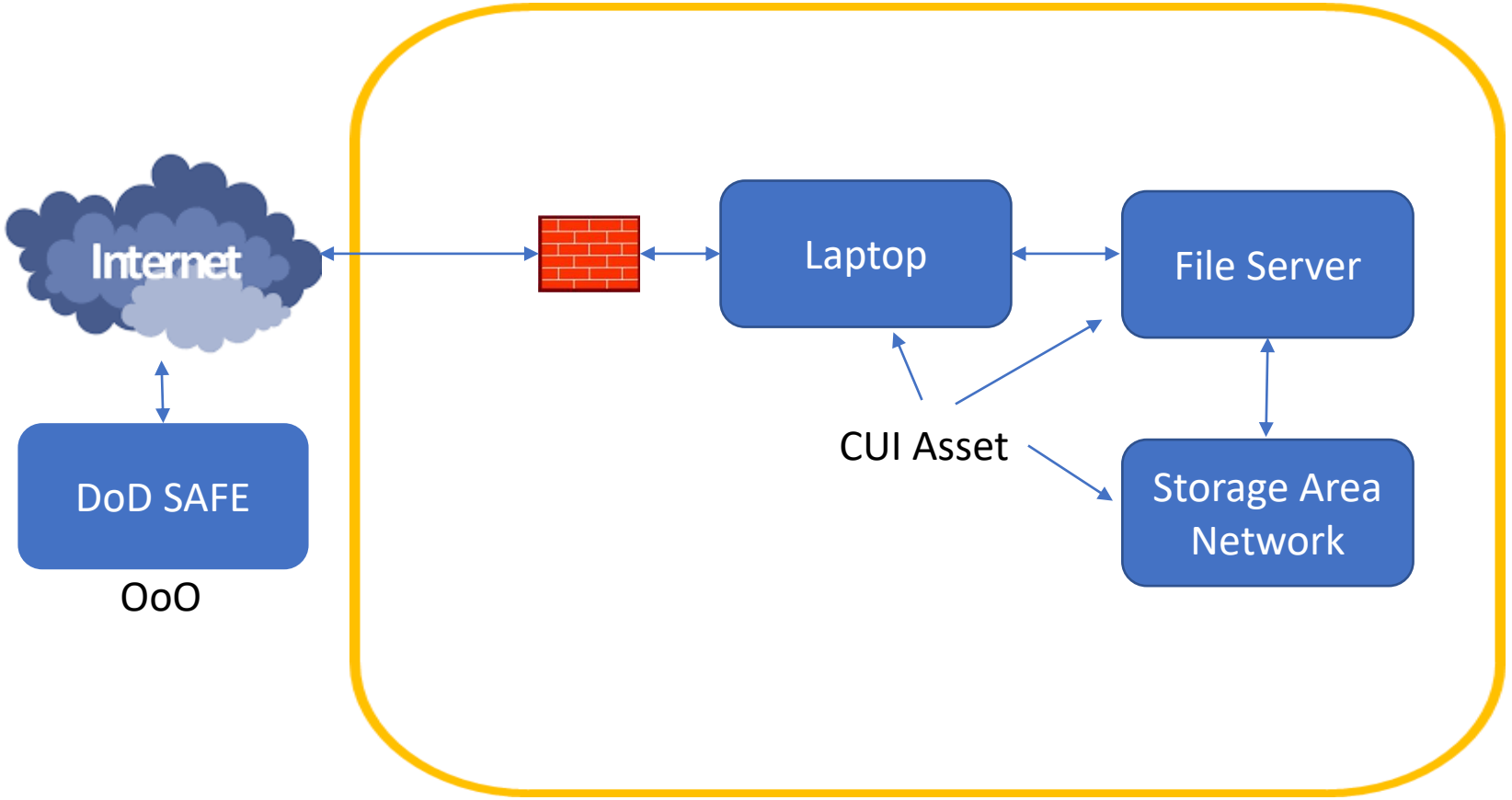
CATEGORIES OF CUI

For information to be considered CUI, it must fall within a category, such as:

- Critical Infrastructure
- Defense
- Export Control
- Financial and Tax
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional *(for DHS use only)*
- Statistical
- Transportation

CUI Data Flows

- Used to map how CUI travels internally and externally



Scoping from NIST 800-171

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms).

.

Assessment Scope for Level 2

- Released Dec 3rd, 2021 CMMC 2.0 Scoping Guidance Level 2

- Established Asset Categories
  - Controlled Unclassified Information (CUI) Assets
  - Security Protection Assets
  - Contractor Risk Managed Assets (CRMA)
  - Specialized Assets
- Out-of-Scope Assets

- Defined Contractor and CMMC Assessment requirements for each Asset Category

Asset Categorization

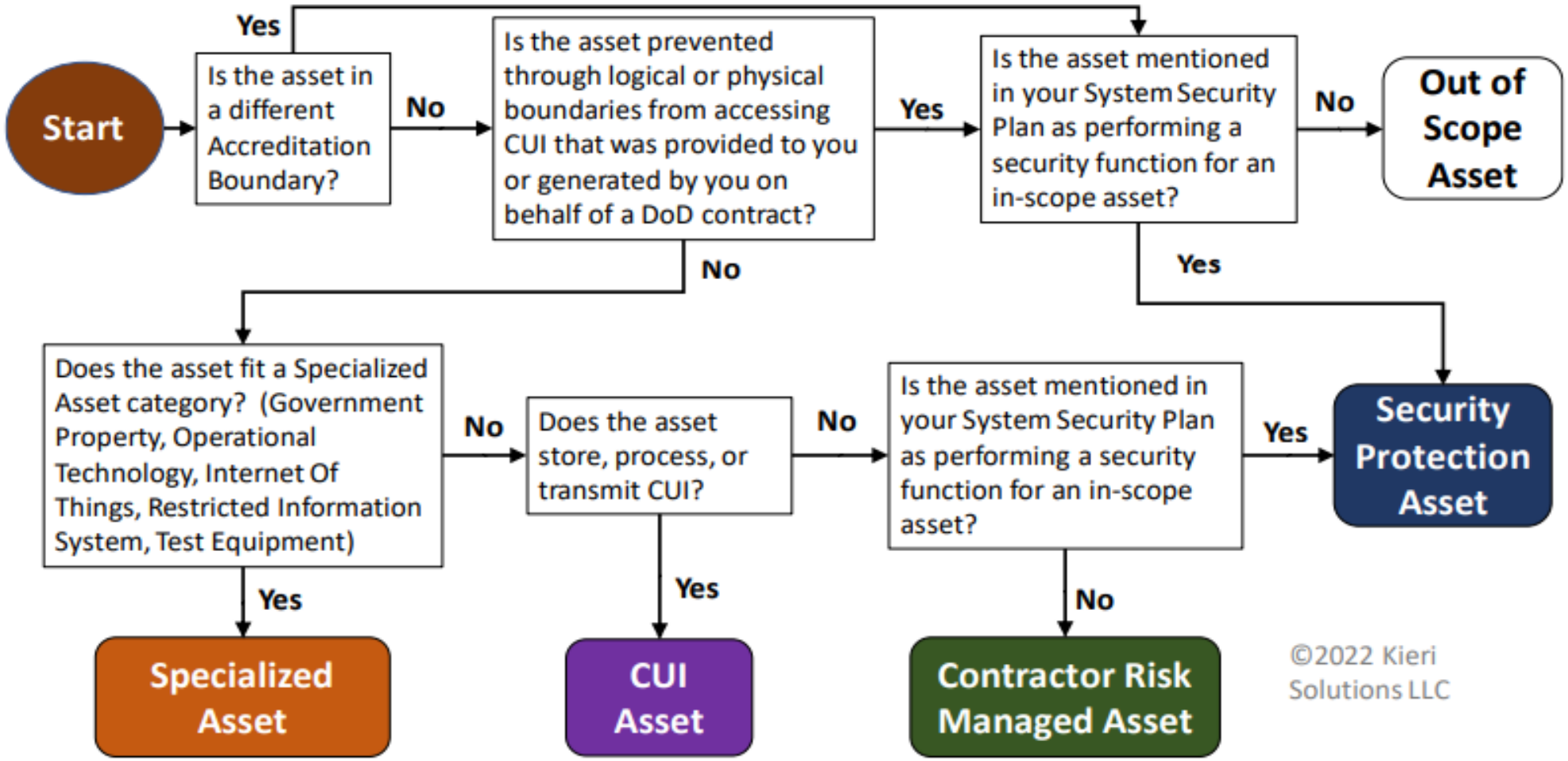
- **Only CUI and Security Protection Assets get assessed against all CMMC Practices**
- **CRMA and Specialized Assets are only assessed against the CA.L2-3.12.4 Practice**
  - **Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.**
  - **Spot checks required for CRMA assets**

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Assets that are in the CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	• Assets that process, store, or transmit CUI	• Document in the asset inventory • Document in the System Security Plan (SSP) • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC practices	• Assess against CMMC practices
Security Protection Assets	• Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI		

Contractor Risk Managed Assets	• Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
	• Assets are not required to be physically or logically separated from CUI assets
		• Document in the asset inventory
		• Document in the SSP
		  ○ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices
		• Document in the network diagram of the CMMC Assessment Scope
			• Review the SSP in accordance with practice CA.L2-3.12.4
			  ○ If appropriately documented, do not assess against other CMMC practices
			  ○ If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks
			  ○ The limited spot check(s) shall not materially increase the assessment duration nor the assessment cost
			  ○ The limited spot check(s) will be within the defined assessment scope

Specialized Assets	• Assets that may or may not process, store, or transmit CUI • Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment		• Review the SSP in accordance with practice CA.L2-3.12.4 • Do not assess against other CMMC practices
Assets that are not in the CMMC Assessment Scope			
Out-of-Scope Assets	• Assets that cannot process, store, or transmit CUI	• Assets are required to be physically or logically separated from CUI assets	• None

Asset Categorization



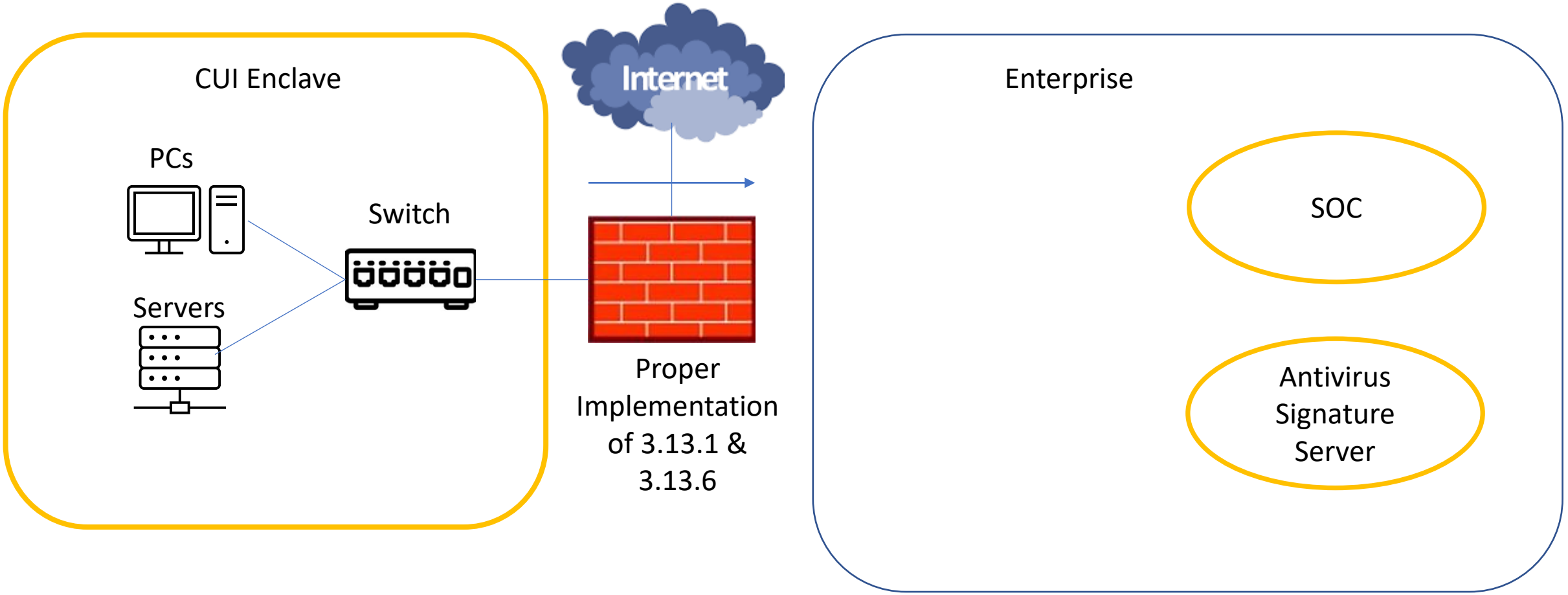
What is an Enclave

- A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.
  - Define by NIST COMPUTER SECURITY RESOURCE CENTER and CNSSI 4009
- This means proper physically or logically isolation from the Enterprise
  - Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms).
  - Use separate Identity and Access Management

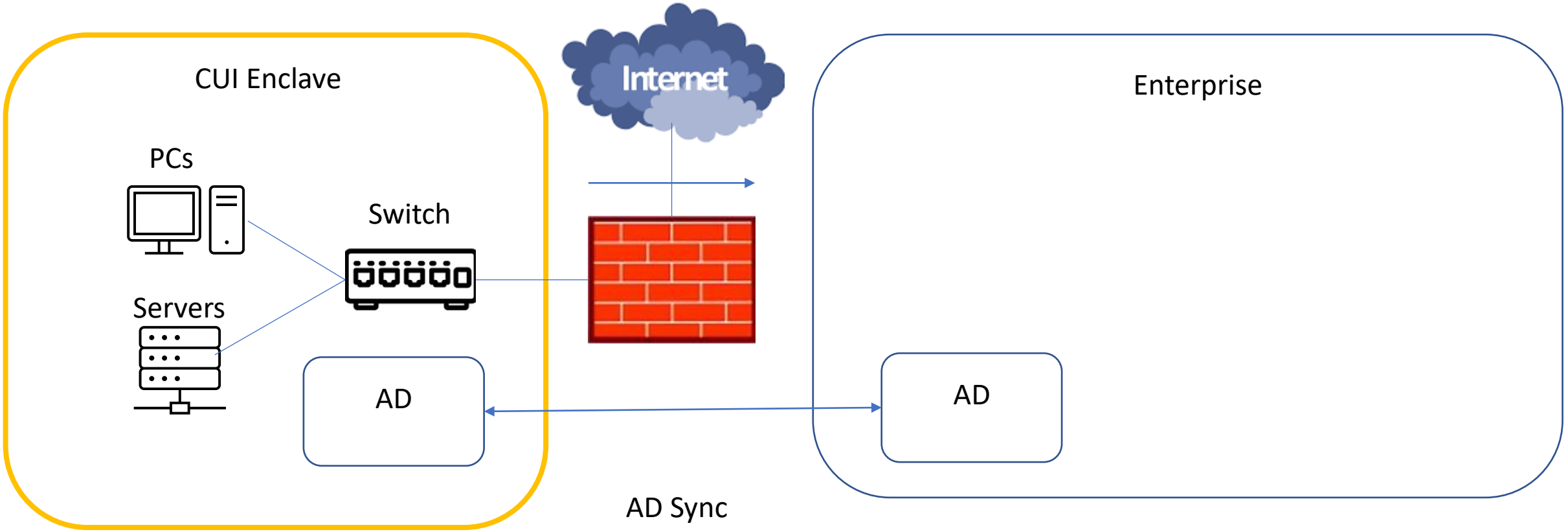
To Enclave or not to Enclave

- Pros
  - Labor to screen and monitor personnel
  - Labor to maintain and monitor security systems
  - Labor to maintain systems (patching)
  - Licenses or purchase cost for security systems
  - Training and managing your staff
  - More likely to pass an audit
  - Concentrate efforts
- Cons
  - Increase in assets/Duplication of efforts
  - Collaboration between Enterprise and Enclave
  - At CMMC Level 2 and above, your users are restricted in what they can do
  - As your scope increases, the skilled labor needed to keep it secure also increases
  - Legacy Systems - Some systems simply cannot meet requirements for CMMC Level 2 and above.

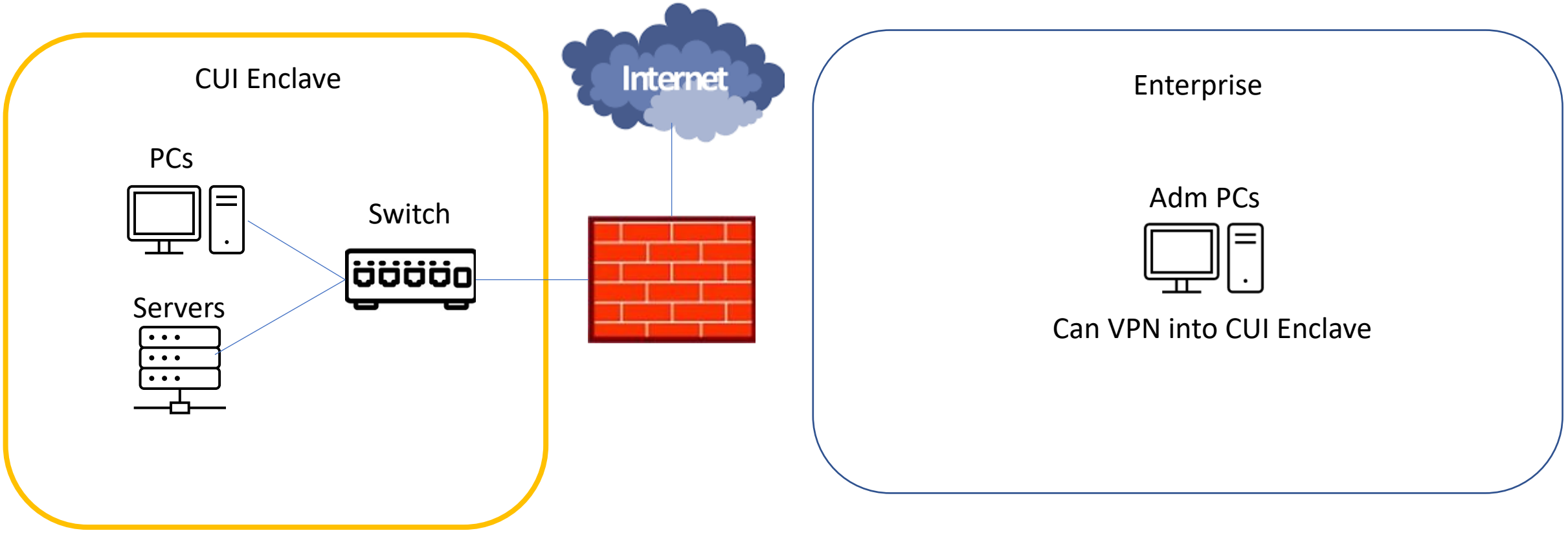
Enclave In Scope assets



Isolation Fails



Isolation Fails



Training

- Security Awareness Training
  - Over 90% of successful cyber attacks start with a phishing email
- Secure your home WiFi
  - Access you Router's setting by typing 192.168.0.1 into your browser
  - Change your default password on your Wireless Router
  - Change the SSID to make it harder to identify the type of router you use – do not use anything that could be used to identify you
  - Limit network access based on MAC address
  - Ensure the Router's firmware is up to date

Contact info: Thad Wellin, CISSP, CCP
twellin@trwsecuritysolutions.com