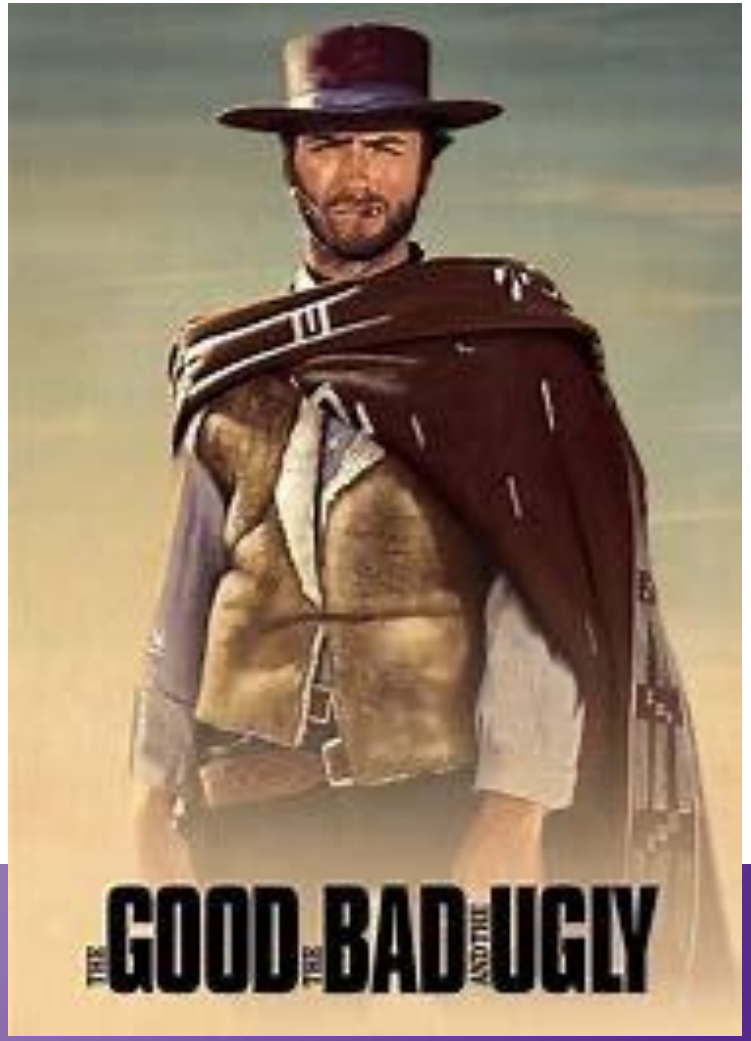
Scoping your Boundary

The Good, the Bad, and the Ugly

Koren Wise – Wise Technical Innovations

Mark DeBry - Shadowscape



Koren Wise

- CEO of Wise Technical Innovations
- **C3PAO,** Lead CCA, PI, CISSP
- Azure Gov / GCCH Secure Enclave Network Architect
- Developed the ***MVP Enclave and 800-171 Compliance Program***
- **Authorized Training Provider** for the CCP & CCA Assessor Program

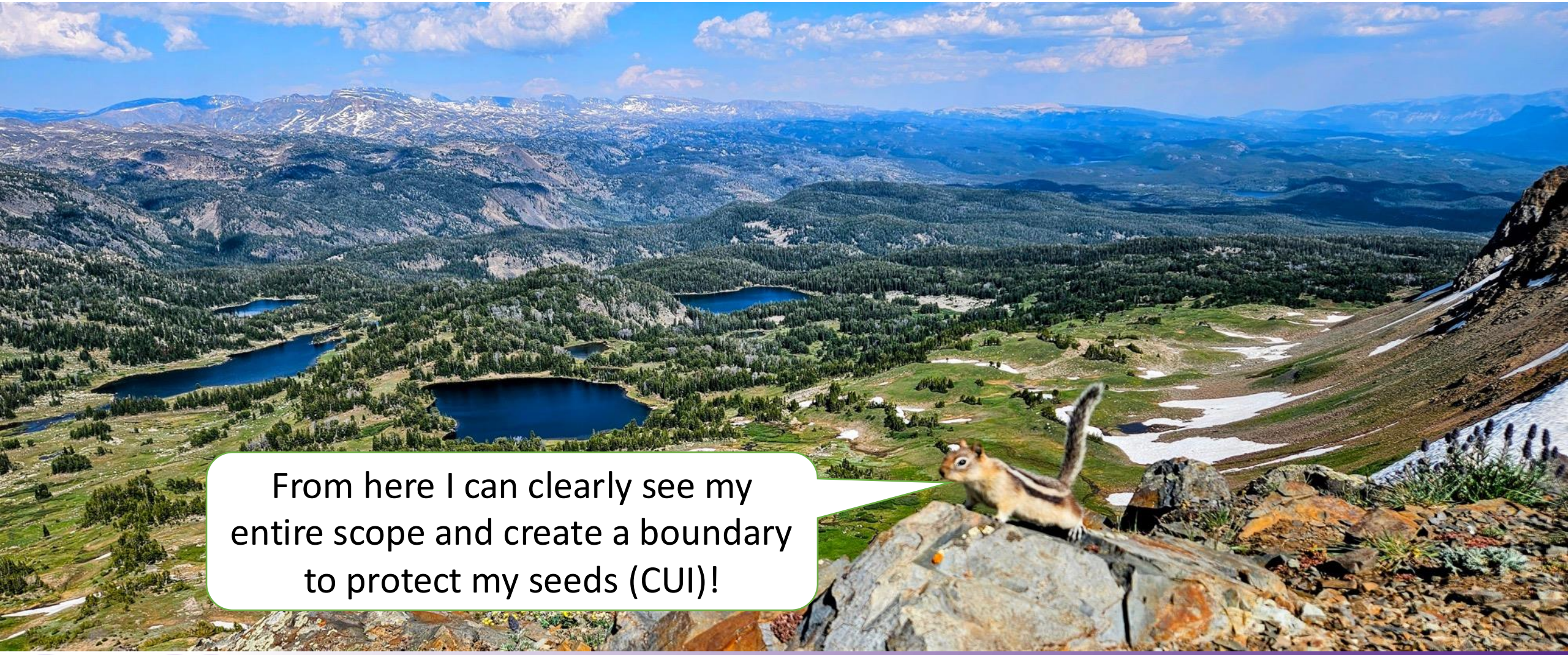
Mark DeBry

- VP of Business Ops at Shadowscape - Security Services, Training, Analytics
- Lead CCA, CISM, PMP
- Assisting companies prepare for L2
- Performing multiple L2 assessments as Lead Assessor
- Microsoft: Director Federal Security
- IBM: Director Global Services Security

Agenda

- Analyze and Define Your Boundary from a 10,000 ft View
- Examples of Protecting CUI with Proper Boundaries
- Set the Stage – Key Terms and NIST Guidance
- Critical Steps to Accurately Scope your Boundary
    1. Identify ALL Your People / Technology / Facilities
    2. Properly Categorize All Your Assets
    3. Develop Comprehensive Network Diagrams showing **BOUNDARIES**
    4. Define External Service Providers (ESP) / Cloud Service Providers (CSP)
    5. Map Data Flows and Data Management
    6. Diagram Logical / Network and Physical Boundaries
    7. Determine Assessment Scope – Enterprise or Enclave
- The Bad and the Ugly: Avoid the Pitfalls
- 4 Key Takeaways

Analyze and Define your Boundary from 10,000ft



Examples of Protecting CUI with Proper Boundaries

- CUI is like Prisoners or Cash – MUST be protected
- Inside the boundary – like a prison or bank – data can move around
- Outside the boundary – protections must be in place for external transport
- If you have holes in your boundary – CUI will leak out

Set the Stage - Key Terms

- **Scope** – The technology, people, and facilities that will be inspected during the assessment of an Organization Seeking Assessment (OSA) .
- **Boundary** - Physical or logical perimeter of a system (NIST GLOSSARY)
- **Boundary Protection Device** - A device (e.g., gateway, router, firewall, guard, or encrypted tunnel) that facilitates the adjudication of different system security policies for connected systems or provides boundary protection. The boundary may be the authorization boundary for a system, the organizational network boundary, or a logical boundary defined by the organization. (NIST GLOSSARY)
- **Internal Network** - A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors. (NIST GLOSSARY)
- **Covered Information System** - Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. (252.204-7012)
- **External** - A network not controlled by the organization (e.g., Internet, ESP, MSP, CSP, Sub) (NIST GLOSSARY)

Design & Implementation

Boundaries

Physical

Logical

Logical and Physical Boundaries

Controlled environment **is any area or space an authorized holder deems to have adequate physical or procedural controls (*e.g.*, barriers or managed access controls) to protect CUI from unauthorized access or disclosure.**

-Title 32 CFR Part 2002

Logical Boundary

Created by things like:

Routers/Gateway Devices (Boundary Protection Device)

L3 Switches

IDS/IPS/Monitoring at Entry/Exit point

Rule Sets

Control of Traffic Flows

"Monitor, Control, Protect"

SC Domain

Physical Boundary

Created by things like:

Doors / Physical Infrastructure

Locks

Badge Readers

Cameras / Monitoring

Visitor Policies

PE Domain

Physical and Logical Boundaries in 800-171

Logical / Network Boundaries

System and Communication Protection Domain (SC)

MUST DEFINE ALL BOUNDARIES IN NETWORK DIAGRAM

- 3.13.1- Monitoring, Controlling, Protecting at external & internal boundaries
- 3.13.5- Public-access system separation
- 3.13.6- Ruleset at boundary must deny by default, use whitelisting

Physical Boundaries

Physical Protection Domain (PE)

Protect organizational systems, equipment, and operating environments

- 3.10.1- Limit Physical Access
- 3.10.2- Monitor Facility
- 3.10.3- Escort Visitors
- 3.10.4- Physical Access Logs
- 3.10.5- Manage Physical Access
- 3.10.6- Alternative Work Sites

CAN process, store, or transmit – In Scope
CANNOT process, store, or transmit – Out of Scope

Assets that CAN	Assets that CANNOT	Assets that CAN but are NOT INTENDED TO
• Systems are in the same logical subnet or VLAN. They are within the same **logical boundary** or there is a lack of a boundary altogether. • People who are inside the physical boundary can see, overhear, or access CUI on systems.	**CANNOT**- Non-CUI Assets are separated from CUI Assets by an effective information system boundary and physical boundary.	**Contractor Risk Managed Assets** are inside the boundary, HOWEVER… • The contractor states they will not process, store, or transmit CUI. • The contractor must still protect using NIST SP 800-171 • Assessors do not assess against all controls if in agreement.

CRITICAL COMPONENTS OF A NETWORK DIAGRAM

1. Network Components

- **Servers** (application, database, file servers)
- **Workstations/Endpoints** (desktops, laptops, mobile devices)
- **Network Appliances** (firewalls, routers, switches)
- **Storage Devices** (NAS, SAN)
- **IoT Devices** (printers, cameras, smart sensors)

2. Network Connections

- **Wired Connections**: Ethernet, fiber optics, or serial connections between devices.
- **Wireless Connections**: Wi-Fi, Bluetooth, or cellular connections.
- **Cloud Services and External Connections**: Connections to SaaS, IaaS, or hybrid cloud environments.
- **Virtual Networks**: VPNs, VLANs, and SD-WANs.

3. Network Boundaries & Security

- **Firewall**: Defines the boundary between the internal network and the internet or external networks.
- **DMZ (Demilitarized Zone)**: A zone that hosts publicly accessible services while keeping the internal network secure.
- **Intrusion Detection/Prevention Systems (IDS/IPS)**: Security monitoring and response mechanisms.
- **Access Control Lists (ACLs)**: Defines security rules governing traffic flow.

4. IP Addressing & Subnetting

- **IP Address Ranges**: Public and private IPs assigned to different devices.
- **Subnetting**: Dividing the network into smaller logical segments for better management and security.
- **VLANs**: Virtual segmentation of networks to isolate traffic.

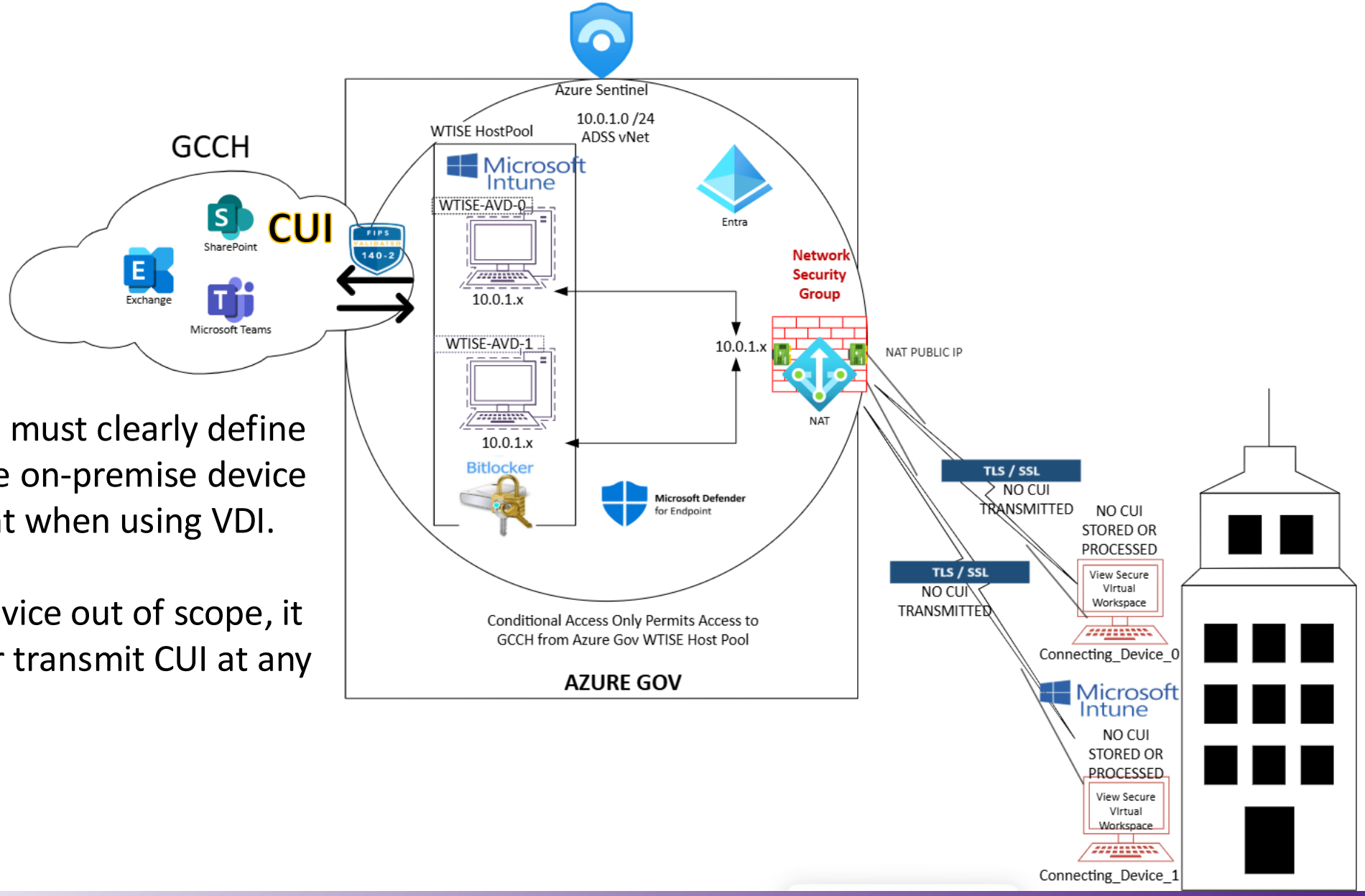
5. Network Topology & Layout

- **Star, Mesh, Bus, Ring, or Hybrid Topologies**: Defines the physical or logical structure of network connections.
- **Data Flow & Communication Paths**: Indicates how data moves between devices and services.

6. Redundancy & Failover Mechanisms

- **Load Balancers**: Distributes traffic among multiple resources.
- **Failover Links**: Secondary connections for redundancy.
- **High Availability (HA) Configurations**: Ensuring uptime with clustered systems.

Popular Scoping Format – “All Cloud / VDI”



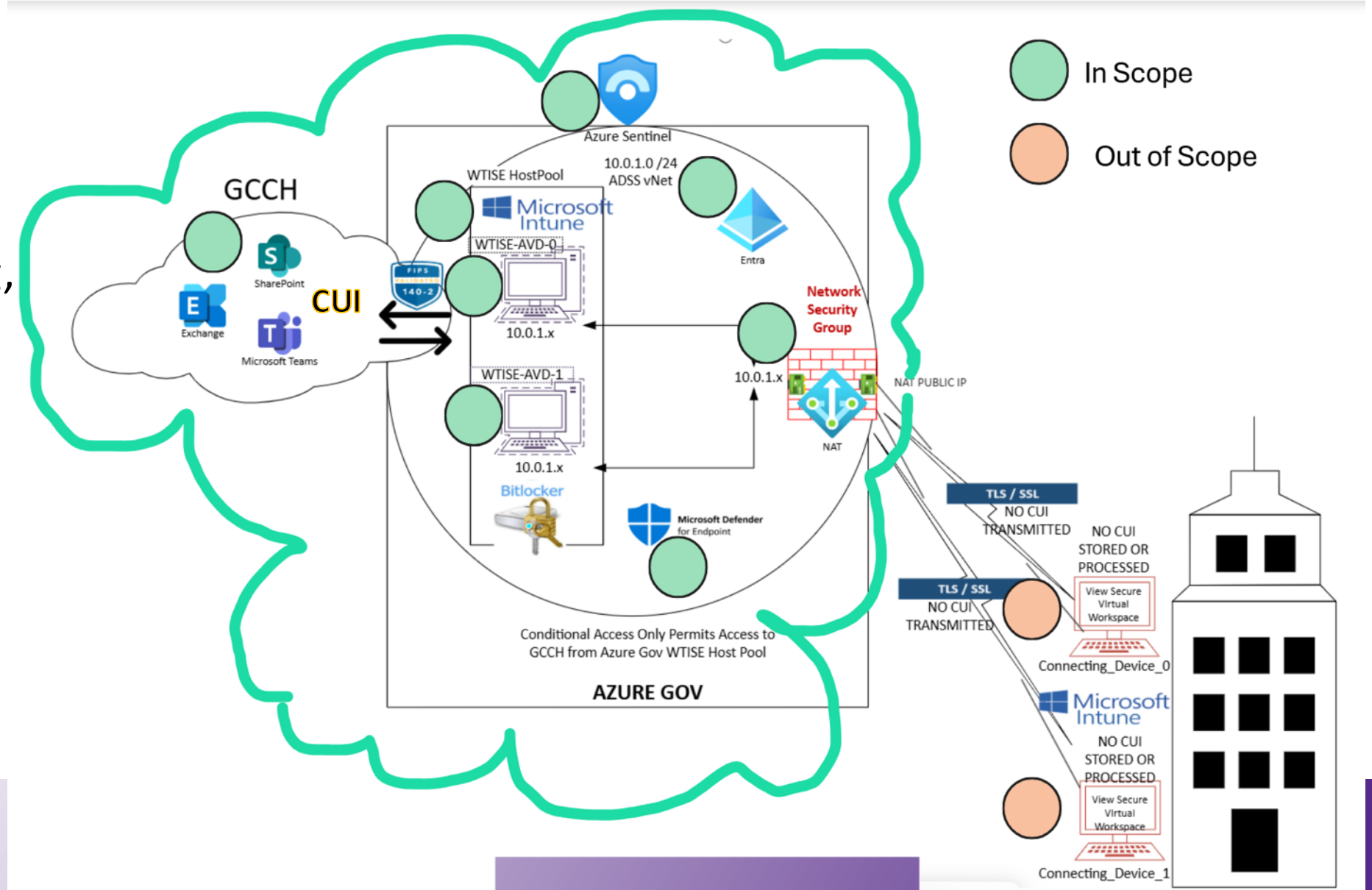
All cloud implementations must clearly define the boundary between the on-premise device and the cloud environment when using VDI.

To keep the connecting device out of scope, it CANNOT process, store, or transmit CUI at any time.

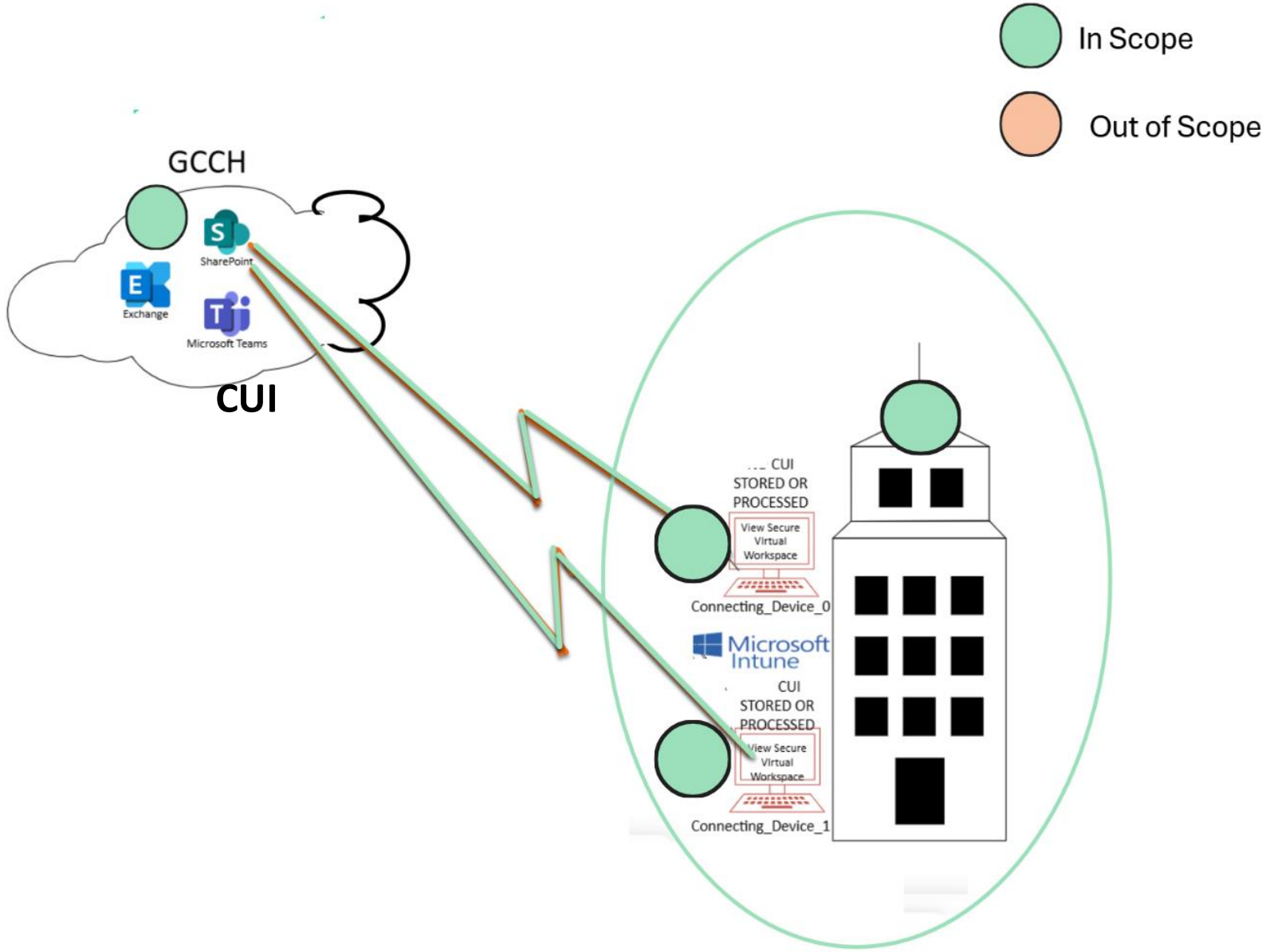
CUI-CON 2025

VDI Configured Environment to Contain CUI

32 CFR Part 170:
An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard / Video / Mouse sent to the VDI client is considered an Out-of-Scope Asset

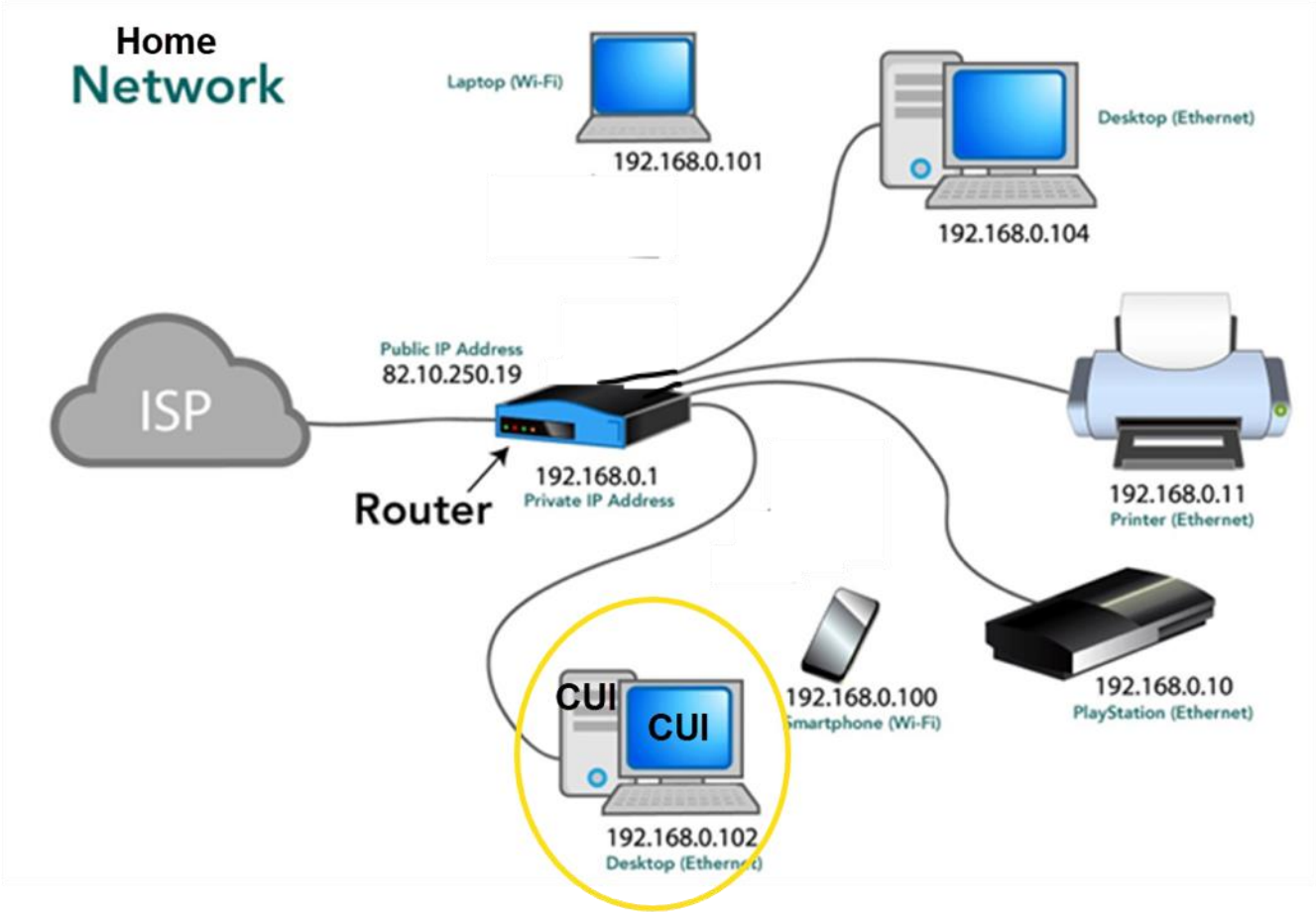


Cloud Configured Such that Endpoint CAN Process Store or Transmit CUI



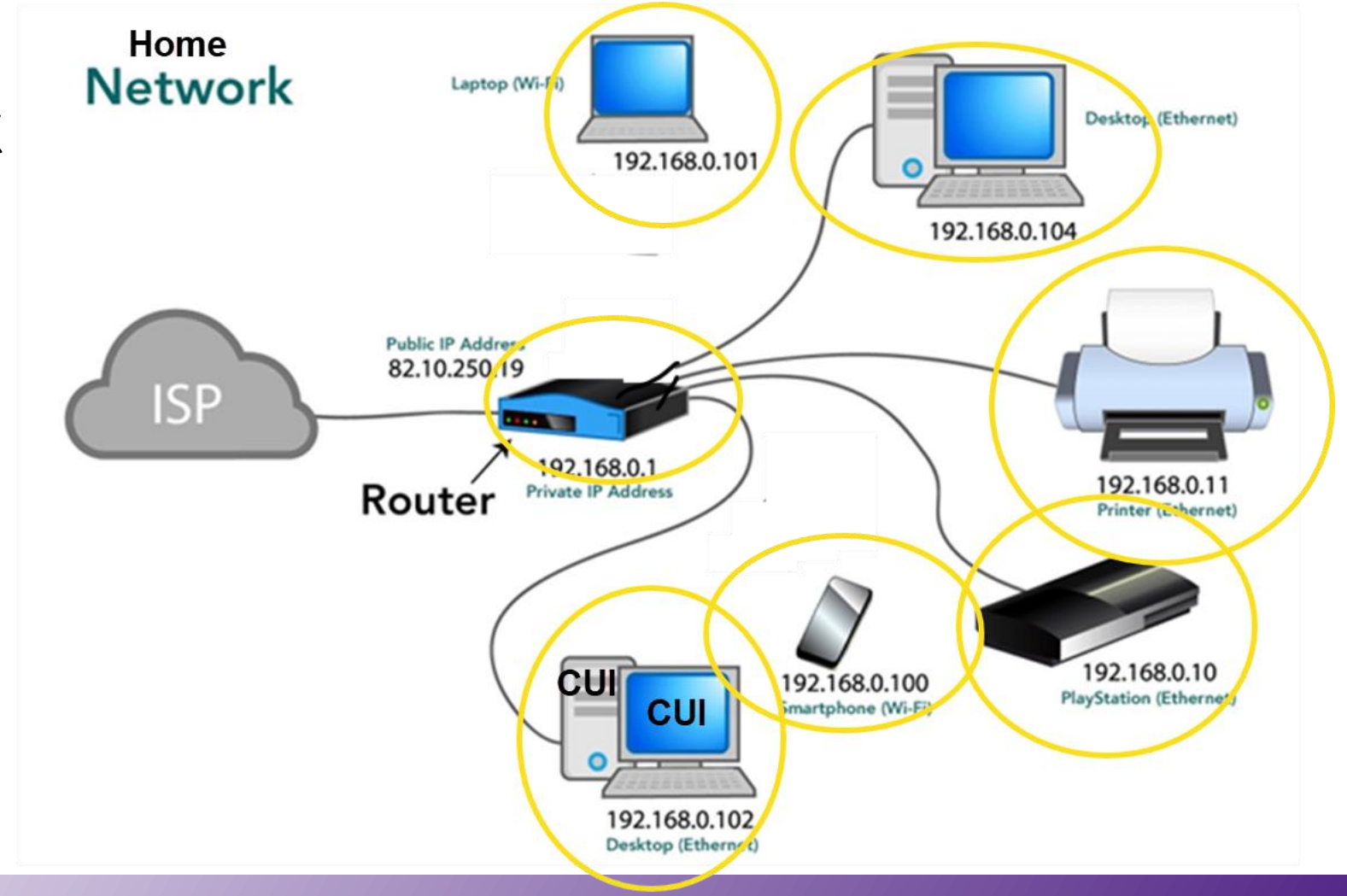
“CAN” Process, Store, or Transmit

There is no network boundary between CUI assets and assets that do not process, store or transmit CUI. Therefore, they all “CAN” process, store, or transmit CUI.

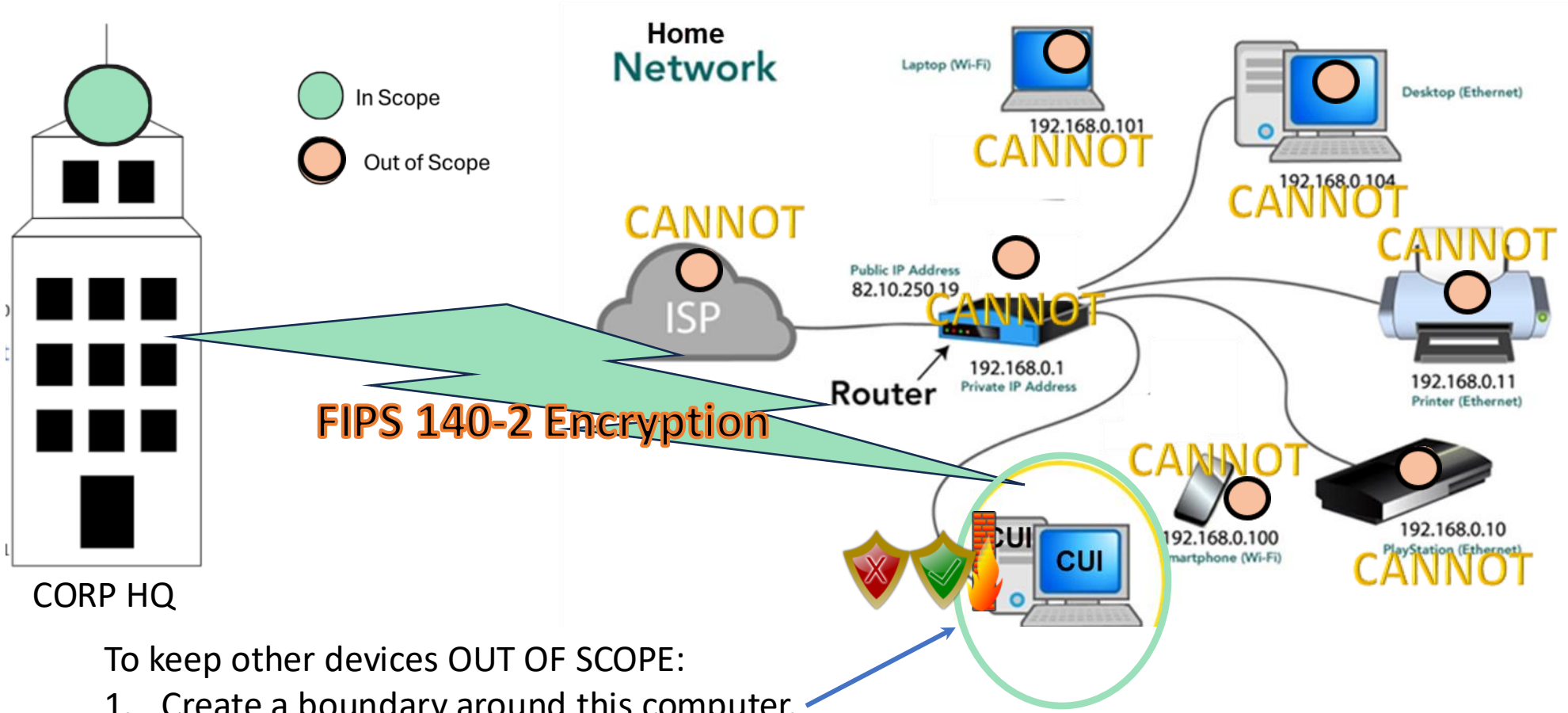


“CAN” Process, Store, or Transmit

There is no network boundary between CUI assets and assets that do not process, store or transmit CUI. Therefore, they all “CAN”



How do I change "CAN" to "CANNOT" Process, Store, Transmit?

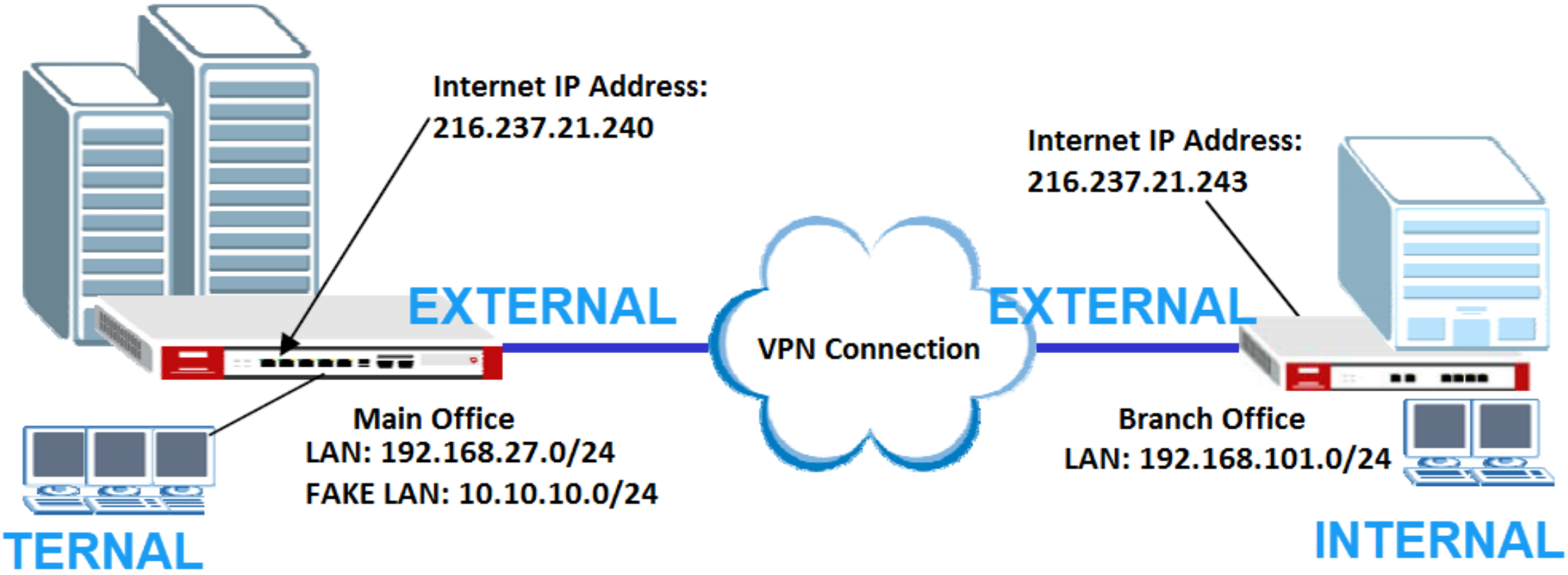


To keep other devices OUT OF SCOPE:

1. Create a boundary around this computer.
2. **REMEMBER: A proper boundary can control, monitor, and protect (3.13.1).**
3. Implement all controls that are applicable to this device in NIST SP 800-171.
4. Address the physical protections using strong Alternate Workspace Policy (3.10.6).

Understanding the Terms Internal and External

- **Monitor, control, and protect communications** (i.e., information transmitted or received by organizational systems) **at the external boundaries** and key internal boundaries of organizational systems.
- External Communication should be protected using **FIPS 140-2 Encryption**

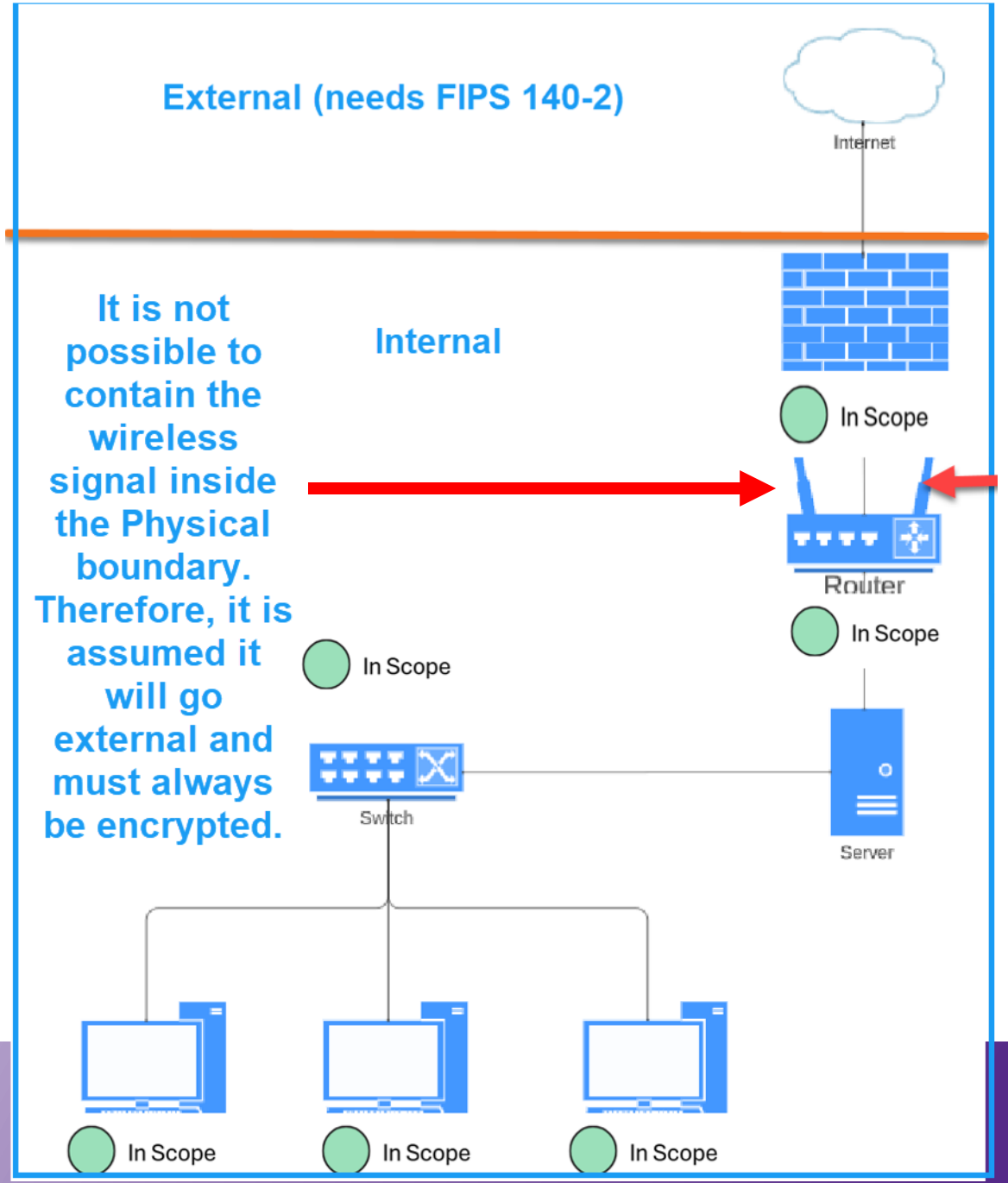


WIRELESS TRANSMISSIONS CANNOT BE CONTAINED INSIDE THE BOUNDARY.

THEREFORE, SUCH CUI TRANSMISSIONS MUST BE ENCRYPTED AT FIPS 140-2.

ALWAYS BE ABLE TO LOOK AT YOUR NETWORK DIAGRAM AND SAY:

"THIS AREA IS INTERNAL"
"THIS AREA IS EXTERNAL"

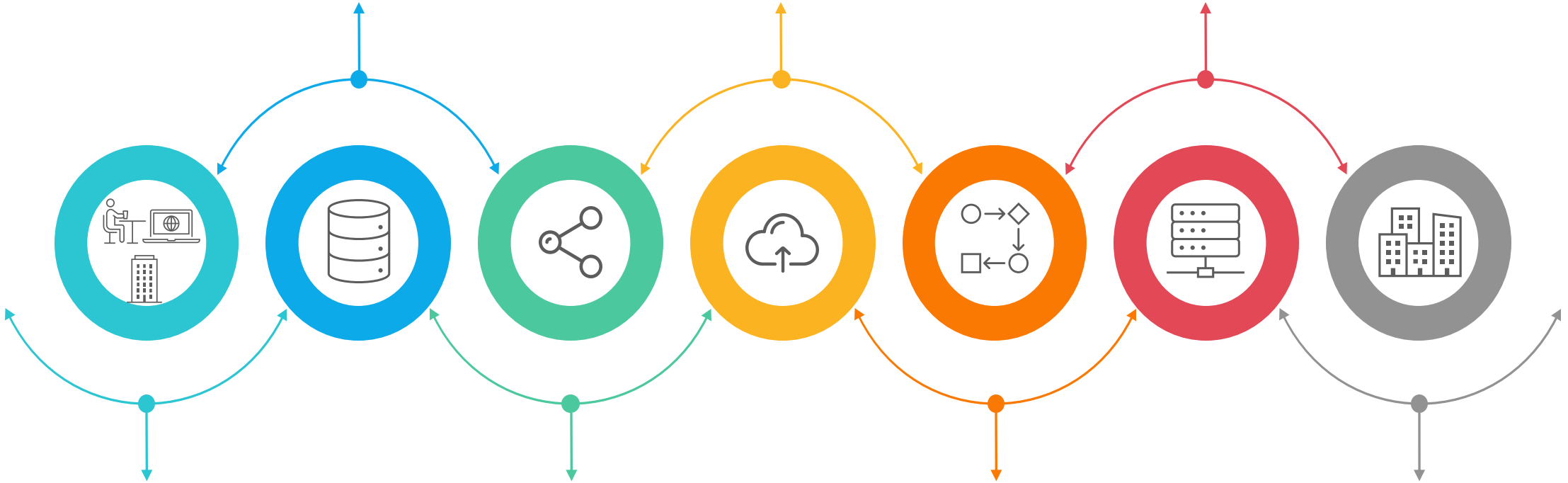


Critical Steps to Accurately Scope Your Boundary

2. Properly Categorize All Your Assets

4. Define External and Cloud Services Providers (ESP/CSP)

6. Diagram Logical / Network and Physical Boundaries



1. Identify ALL Your People / Technology / Facilities

3. Develop Comprehensive Network Diagrams

5. Map Data Flows and Data Management

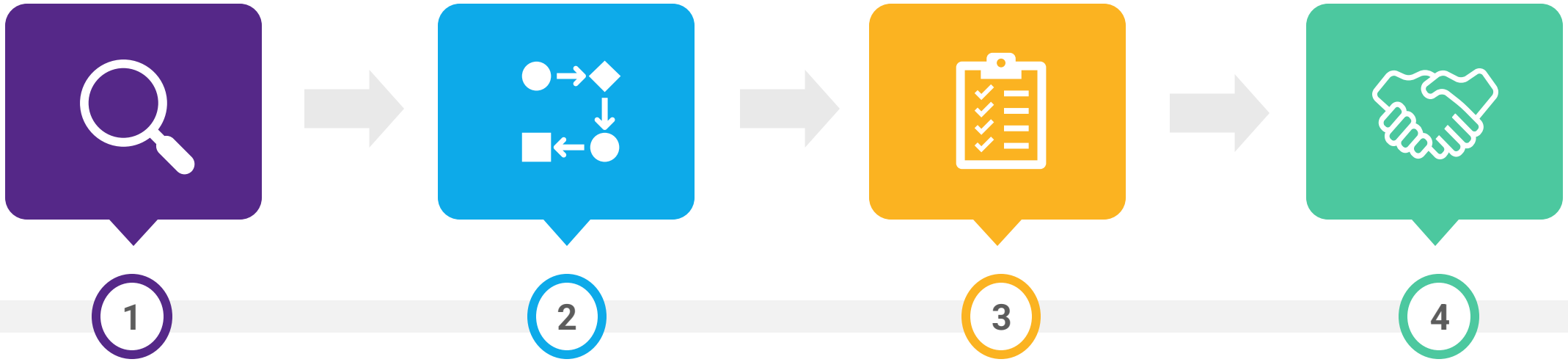
7. Determine Assessment Scope – Enterprise or Enclave

THE BAD AND THE UGLY: AVOID THE PITFALLS

Technologies that easily create unintended scope expansion or leave CUI unprotected:

- Unidentified Assets – Identify ALL
- Emailing CUI without end-to-end FIPS 140-2 Encryption
- FIPS Validated Devices – Protect the Boundary
- Wireless without FIPS – Data Leakage
- Alternate Workspaces (e.g., home) – Without proper boundaries and controls
- Mobile Phones – In Scope if Access to CUI
- ESP/CSPs – Help or Hurt You?
- Subcontractors – You're Responsible
- Enclave – Scope Creep

4 Key Takeaways



1

Identify All

You **CANNOT** protect what you don't know about your environment, data flows, and ESPs.

2

Follow the Process

The concepts to properly define your scope and boundaries build on each other.

3

Clearly Articulate

Network diagrams and data flows clearly define your scope and boundaries.

4

Ask for Expert Advice

This is complex – ask for help to define and validate you've accurately scoped your boundaries.

Bonus: Implications

- Assets in the same network boundary as CUI assets will be in scope.
- People inside the same physical boundary with digital CUI, CUI assets, or other CUI media will need to authorized and will be in scope.
- Visitors must be monitored and escorted inside the physical boundary.
- Care must be taken to never work with CUI without the proper protective boundaries in place.

Bonus: Properly Categorize All Your Assets

In Level 2 assessment, assets are mapped into 1 of 5 categories as defined in 32 CFR

Asset Category	Asset Description	OSA Requirement
CUI Assets (CUIA)	Assets that **CAN** **process, store, or transmit** CUI	• Document in **Asset Inventory, System Security Plan (SSP), & Network Diagram** • Prepared to be assessed against **CMMC Level 2 security requirements (except SA)**
Security Protection Assets (SPA)	**Provide security functions or capabilities** **CAN** or **CAN NOT** process, store or transmit CUI	
Contractor Risk Managed Assets (CRMA)	• **CAN**, but are **not intended to** process, store, or transmit CUI • **Not** required to be **physically or logically separated** from CUI assets	
Specialized Assets (SA)	Assets that **CAN** process, store, or transmit CUI but are **unable to be fully secured**, including: IoT*, IIoT, OT, GFE, RIS, & Test Equip	

CUI-CON 2025

*Internet of Things (IoT), Industrial Internet of Things (IIoT), Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems (RIS)

Bonus: Properly Categorizing All Your Assets

In Level 2 assessment, assets are mapped into 1 of 5 categories as defined in 32 CFR

Asset Category	Asset Description	Org Seeking Assessment Requirement
Out-of-Scope Assets	• **CAN NOT process, store, or transmit CUI**; and **DO NOT provide security protections for CUI Assets** • **Physically/logically separated** from CUI Assets • **Endpoint hosting a VDI client** configured to not allow processing, storage, or transmission of CUI	**Prepare to justify the inability** of an Out-of-Scope Asset to store, process, or transmit CUI

Koren Wise

- CEO of Wise Technical Innovations
- **C3PAO,** Lead CCA, PI, CISSP
- Koren@wtinetworks.com
- www.linkedin.com/in/koren-wise

Mark DeBry

- VP of Business Ops at Shadowscape
- Lead CCA, CISM, PMP
- mark.debry@shadowscape.io
- www.linkedin.com/in/markwdebry

Part 2 – Coming Soon

We'll be taking it up a notch! In an upcoming webinar, we'll apply these concepts to CRMA, SPA, SA, and complex ESP scenarios. Stay tuned for details—connect with us on LinkedIn to catch our future post with the date and time!