Cybersecurity Maturity Model Certification (CMMC) Assessment Boundary Scoping

November 9, 2022







Introduction

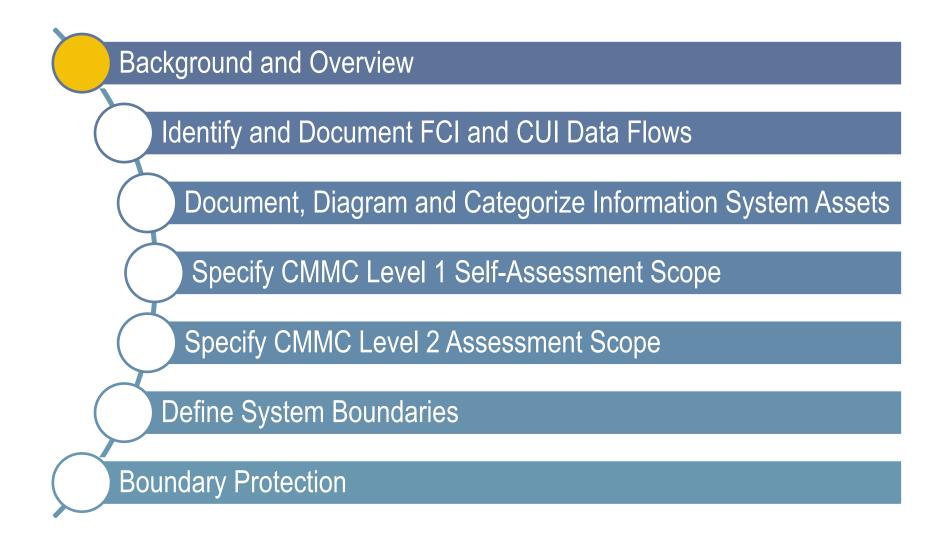
Carly Logan

- CMMC Provisional Instructor
- CMMC Provisional Assessor
- Certified CMMC Professional
- CISSP, CCSP, CRISC
- Senior Auditor and Advisor @ Gray Analytics, Inc.

Background

- ORNL Cyber Risk Management & Oversight
- DOE Cyber-Forensics Lab (JC3) Cyber Program
- DOD DC3 CTA Instructor/Researcher

Cybersecurity Maturity Model Certification Pre-Assessment Training



Background and Overview

Public Information

Public Information or information marked for public release.
Minimum Security Requirements in a nonfederal information system: None

Confidential
Business
Information
Financial, technical and personal information on company systems

Federal Contract Information (FCI)

Information that is not marked as public or for public release Minimum Cybersecurity Requirements in a non-federal information system:

FAR 52.204-21

CUI

Unclassified & not publicly releasable because a specific regulatory or legal requirement requires its protection.

FCI

15 Basic FAR= 17 NIST 800-171= CMMC Level 1

> Contracts after they are issued and associated contract files

RFP responses if responses include detail that is not publicly available such as that which may be described in past performance.

CUI

DFARS 7012+ 110 NIST 800-171 CMMC Level 2

CUI Basic – CUI Specified

Controlled Defense Information (CDI)

Controlled Technical <u>Infor</u>mation (CTI)

Export Controlled
Data
(ITAR/ECI/EAR)

Background and Overview

Public Information

Public Information or information marked for public release.
Minimum Security Requirements in a nonfederal information system: None

Confidential
Business
Information
Financial, technical and personal information on company systems

Federal Contract Information (FCI)

Information that is not marked as public or for public release Minimum Cybersecurity Requirements in a non-federal information system: FAR 52.204-21

CUI

Unclassified & not publicly releasable because a specific regulatory or legal requirement requires its protection.

All CUI is FCI but Not all FCI Is CUI

Background and Overview

DFARS 252.204-7012 "Born"

•

Thou Shalt Protect CUI & apply NIST 800-171

DFARS 252.204-7019 "Crawl"

•

Thou Shalt Enter Self-Attestation in SPRS

DFARS 252.204-7020 "Walk"

•

DIBCAC: "We Shall Trust But Verify"

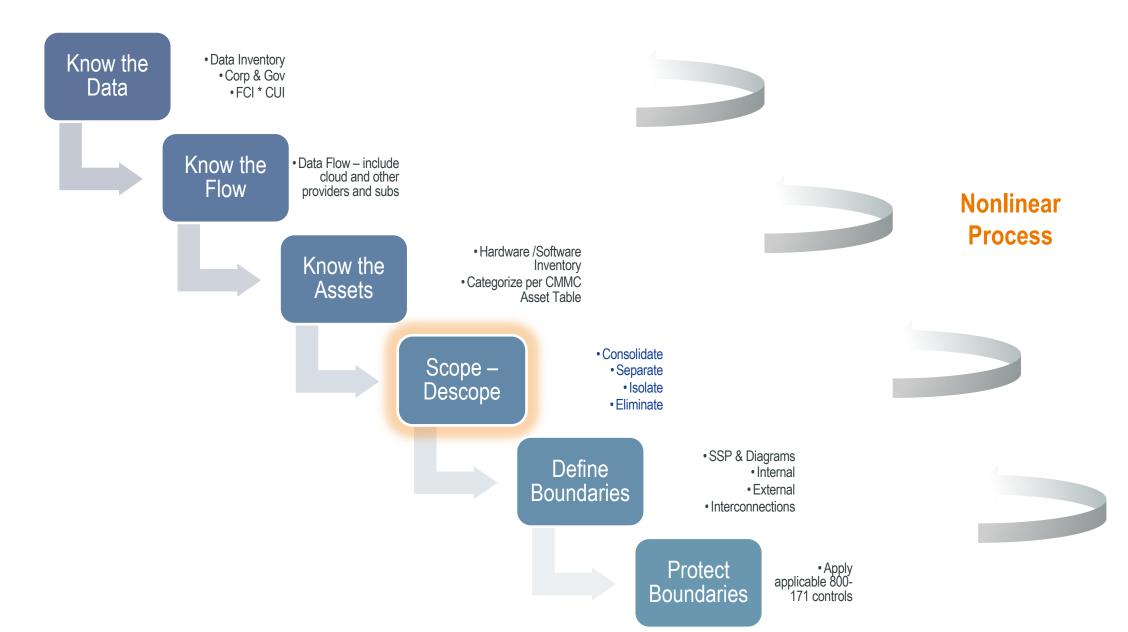
DFARS 252-204.7021 "Run"

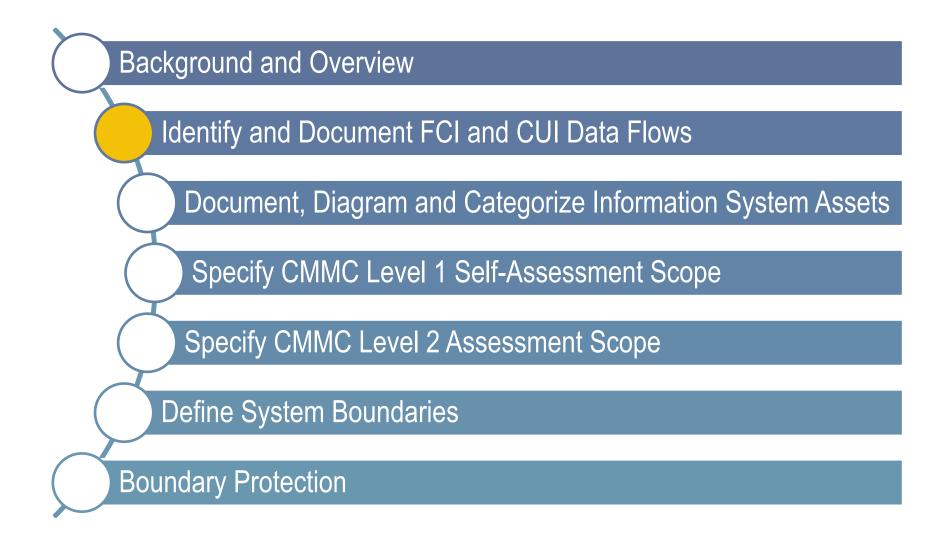
-

3rd Party Assessment. Certification At Time of Award

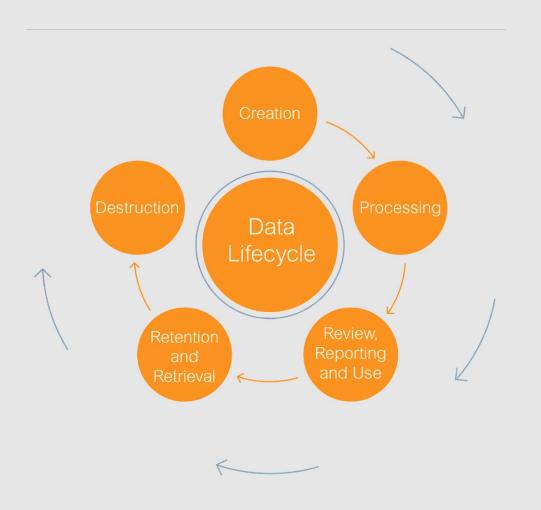
We are HERE

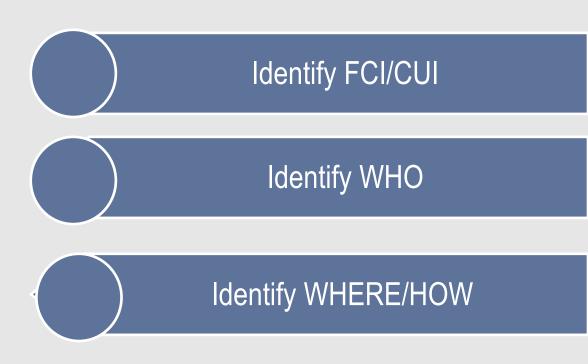
Overview – Determining What is "In Scope" for CMMC





Consider the typical data lifecycle.





Consider the people, processes and technology.

Identify FCI/CUI

Consider the people, processes and technology in the data lifecycle.

Identify and inventory all federal government data the company handles or plans to handle.

- Look at existing <u>contract language</u>, <u>drawings/markings</u>, and the <u>NARA registry</u>.
- Is DFARS 7012 with other CUI or Regulatory language in the contract?
- Is the data ITAR or other ECI?
- Are documents labeled CUI or Controlled Unclassified Information?
- Is information marked with "Distribution B-F?"
- Does data match the NARA Registry CTI, CIS, NNPI, UCNI?

Identify WHO Handles It

Consider the people, processes and technology in the data lifecycle.

Consider how, where and by whom data is processed, stored and transmitted & shared

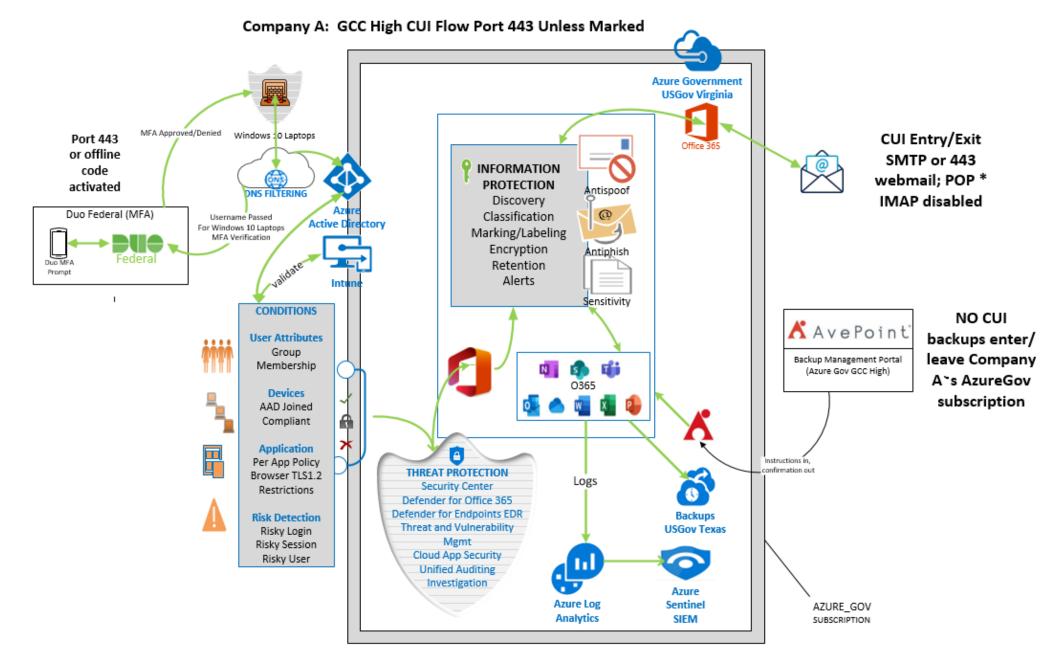
- People Employees, contractors, vendors, external service provider personnel and government customers, DoD, Primes? Subs? Who is the data shared with?
- <u>Technology</u> Servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems & who manages them
- <u>Facilities</u> Physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms and who has access
- **External Service Providers (ESP)** External people, technology, or facilities that the organization uses, including cloud service providers, co-located data centers, hosting providers, MSPs and MSSPs.

Identify WHERE/HOW What Assets

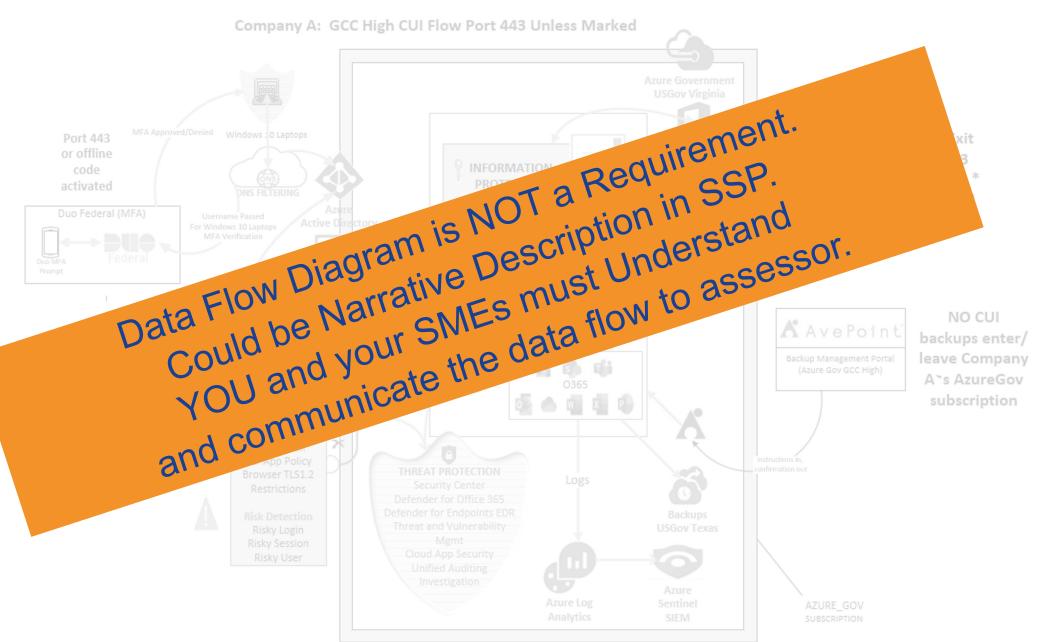
Consider the people, processes and technology in the data lifecycle.

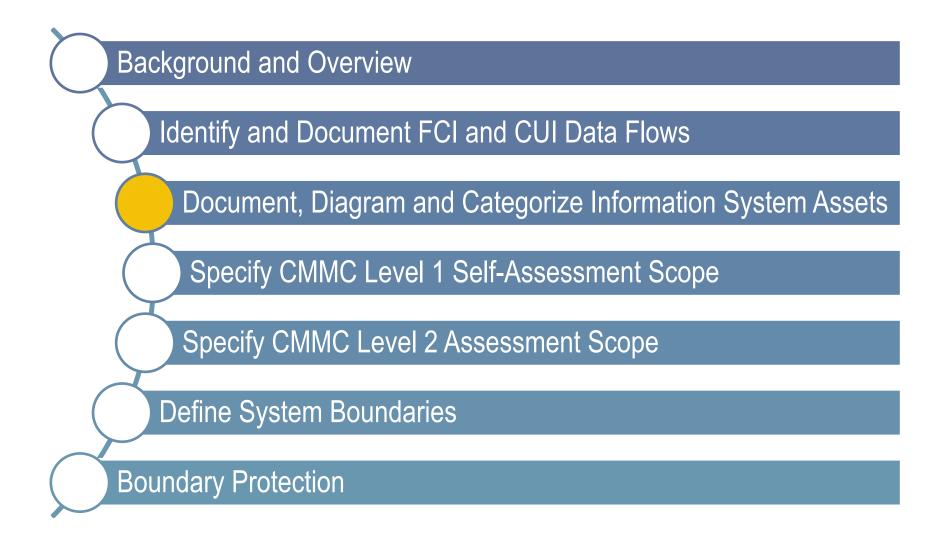
- Where/How: On which user <u>devices</u>, over what internal <u>network segments</u> and devices, or across <u>external networks</u>, using what <u>applications</u> or <u>services</u>, websites, methods does the company receive, generate, process, share, store, transmit, archive (<u>backup</u>) and <u>dispose</u> of FCI or CUI?
 - Exostar? DoD Safe? Prime contractor drop-off? SFTP? File Shares? Email? HardCopy?
- How is FCI or CUI printed? On which printers?
- When is FCI or CUI stored in hardcopy/file cabinets?
- Where are they?
- Where does it go for final disposition? Shredder? Drive Destruction by IT?
- How does Telework/Remote Offices/Alternate Sites affect the DATA FLOW?

Sample Data Flow



Sample Data Flow





Identify and Inventory all assets.

Data Inventory

> Corporate Data

> > FCI

CUI

Hardware Inventory

Include Firmware

Servers, Workstations

> Mobile Devices

Network gear

Software Inventory

Include OS w/version

Applications

Browsers

Office apps

Antivirus

Third Party Provider List

External Providers

MSP/MSSP

Don't forget these assets!

- All the people that use or access the hardware, software, and facilities
- All the physical facilities
 that house all the rest

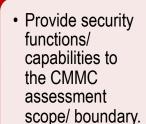
There are 5 CMMC 2.0 Asset Categories

1. CUI Assets

 Assets that process, store. or transmit CUI and are not Security Protection or Specialized **Assets**

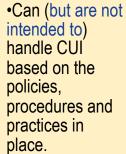
- Workstations
- Servers
- Backup Drives
- AWS S3 Storage
- On-Prem Exchange
- OneDrive/O365

2. Security **Protection Assets**



- May or may not handle CUI.
- May or may not be on same physical/logical segment as CUI assets.
- Vulnerability Scanners
- SIEM/SOC
- Network Admins
- Facility
- M365 Defender

3. Contractor Risk **Managed Assets**



•Mav be on same segment as CUI assets.

- Government property
- IoT devices
- OT devices
- Restricted Information System
- Test Equipment

4. Specialized **Assets**

- Non-traditional IT assets that connect to other systems such as R&D. ICS. SCADA.
- Mav/mav not handle CUI
- May be on same physical/ logical segment as CUI assets.
- Legacy workstation with custom software that can't be updated
- Marketing Dept staff & laptops who don't access CUI

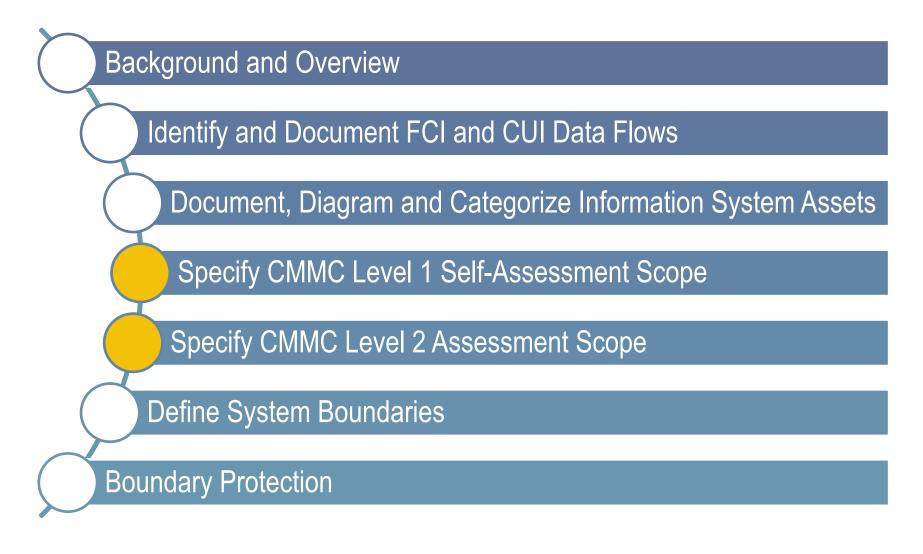
5. Out of Scope **Assets**

 Assets that cannot process. store, or transmit CUI and are logically or physically segregated from CUI assets.

External Service Providers

- In-Scope if access, process, store or transmit CUI
- In-Scope if provide security protection functions or capabilities to CMMC Environment
- Otherwise, Out of Scope

All are In-Scope Assessed against CA.L2-3.12.4 Contractor **Specialized Risk Managed Assets Assets** Include in Asset inventory lists ✓ Include in network diagram ✓ Include in SSP ✓ Include description of how asset is protected through technical or procedural controls **Security CUI Assets** Protection **Assets** Assessed against all 110 NIST 800-171 Requirements



FCI Scope CAN be Different from CUI Scope

CMMC Level 1
Scope
Self-Assessment

Does Enterprise or HQ handle FCI?

CUI Zone, Enclave, Host Unit

FCI Information

is not marked as public or for public release.

Minimum cybersecurity requirements in a non-federal information system:

Basic Safeguarding Clause 48 CFR 52.204-21.

CUI Information

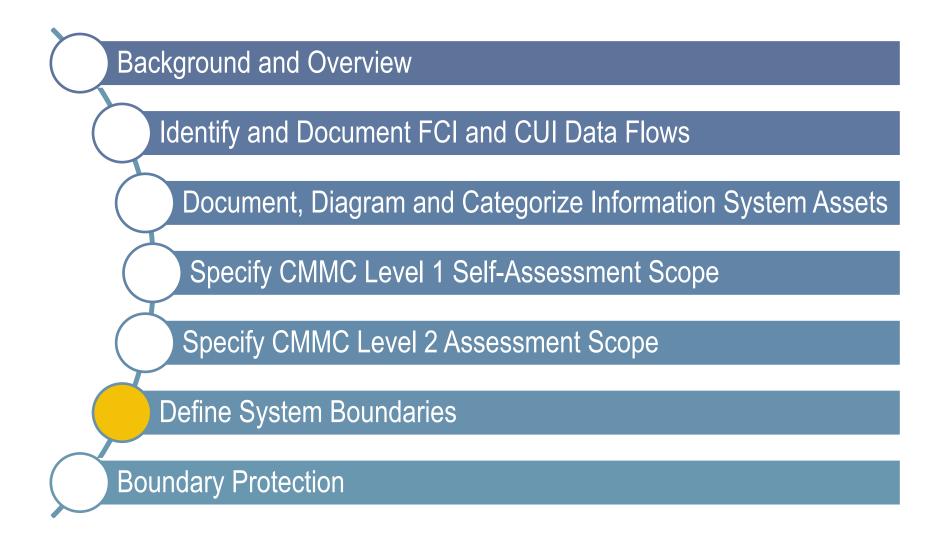
that is marked or identified as requiring protection under the CUI program.

Minimum security requirements in a non-federal information system: NIST SP 800-171.

CMMC Level 2 Scope C3PAO

Can you "Skinny the CUI Scope?"

CUI Zone, Enclave, Host Unit



What are Boundaries?

Assessment Boundary

Defines the in-scope assets and external service providers against which an assessor will evaluate conformity with applicable CMMC practices. This is the boundary for which a CMMC certificate will be applied.

An "Information System" in this context is the collection of assets that are combined and documented in a system security plan (SSP) that describes the assets, data flow, network, internal and external boundaries and connections to external systems outside of those boundaries. (SSP is required for CMMC Level 2 and 3)

External Information System (or component)

A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

May be IN SCOPE for CMMC.

Ex: External SOC or SIEM solutions are now "Security Protection Assets" even if they do not process, store or transmit CUI. Cloud services must be FedRAMP or FedRAMP-equivalent.

Boundary & Boundary Protection

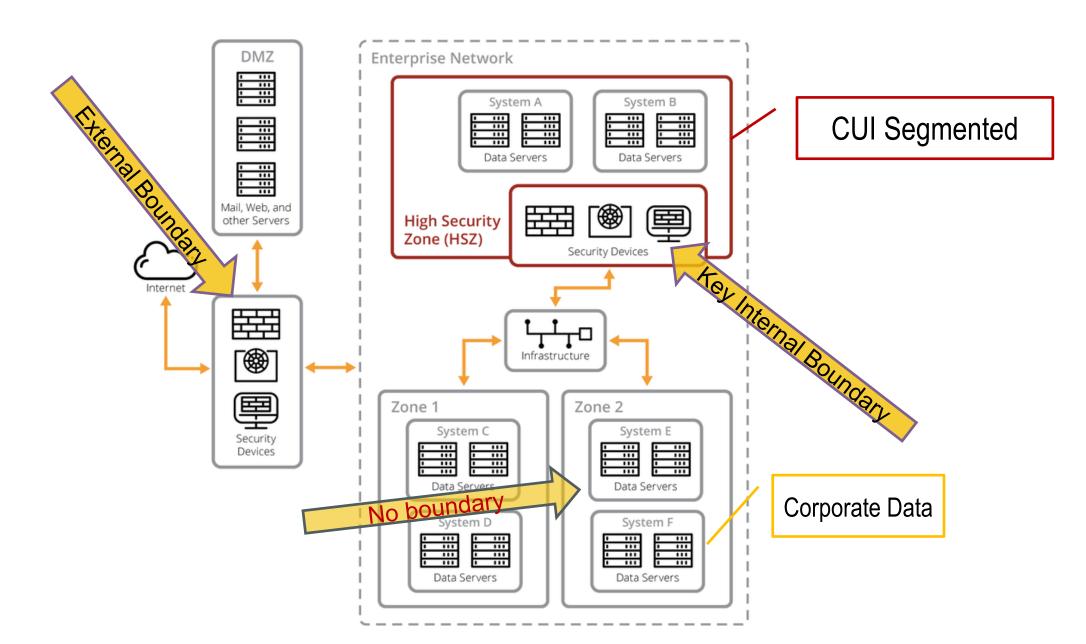
Physical or logical perimeter of a system.

NIST 3.13.1: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of information systems (purpose: to prevent and detect malicious and other unauthorized communications using boundary protection devices.)

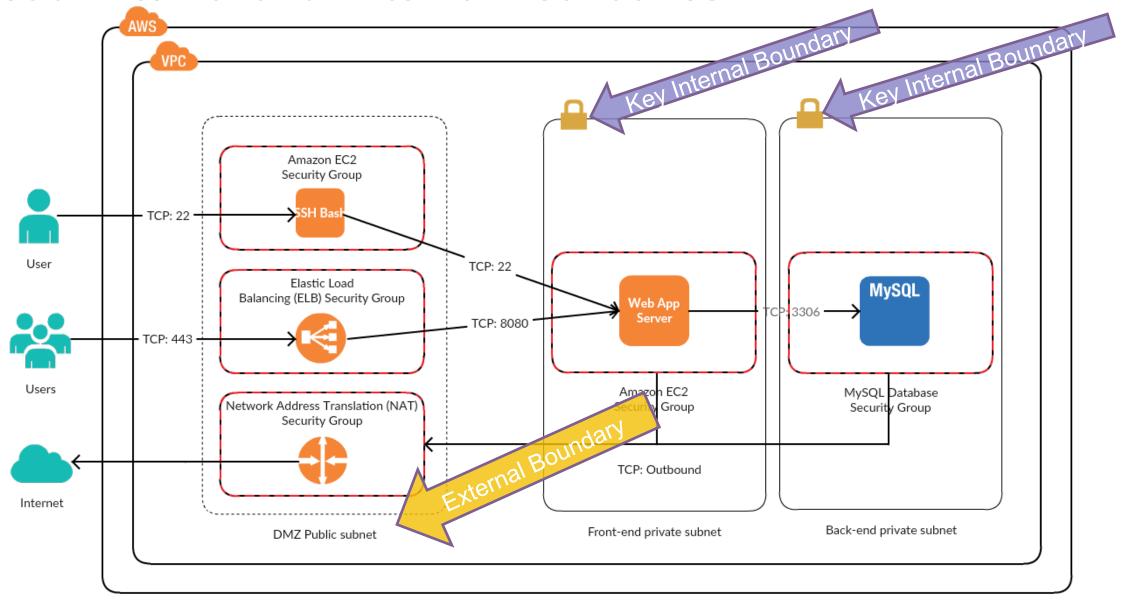
Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.

A boundary is used to prevent CUI from leaving in-scope assets without permission.

Diagram: On-Premises Internal and External Boundaries



Cloud: Internal and External Boundaries

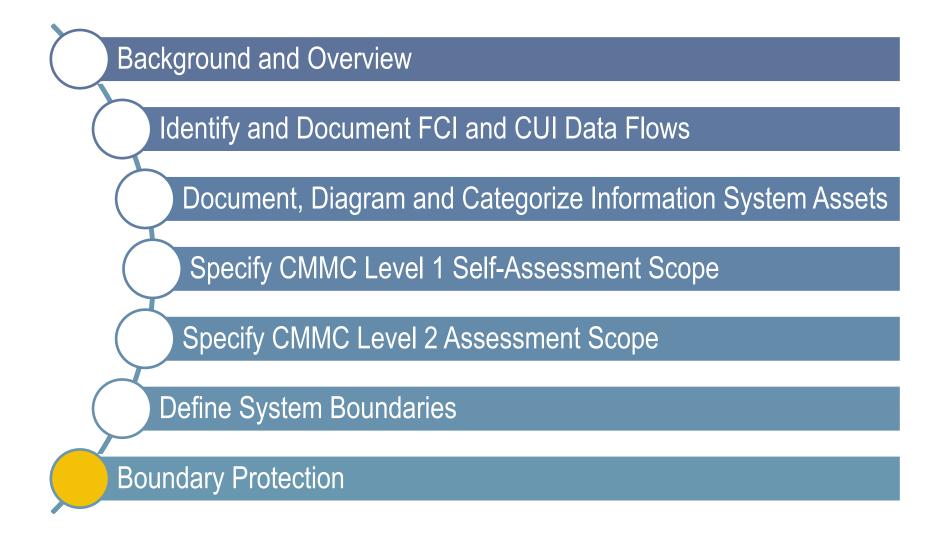


Assessment Scope and Assessment Boundary Recap

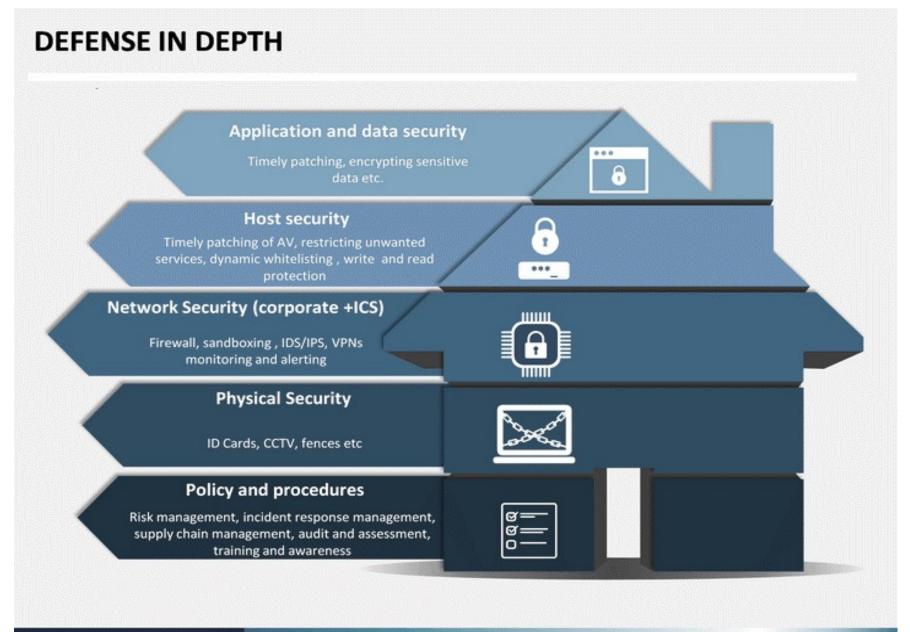
☐ We have determined what is being protected and which NIST 800-171 practices are required. (data and asset inventories) ☐ We have and can draw an invisible circle around all the assets, services, network segments, devices, applications, external providers, etc. that are part of the system "handling" the CUI. (assessment boundary) ☐ We have identified the physical and logical internal and external boundaries, be it a facility or office, borders between the Internet and the internal network, or between internal network segments. ☐ We have documented "interconnections" (external connections to systems outside the Assessment boundary.) ☐ We have updated the system description, diagrams, and mapped out the data flows. ☐ Important: We have also determined what the system manager does and does not have control over. And who IS responsible (i.e., another external system, cloud provider, etc.)

Be sure to document who is responsible for which controls in a

shared responsibility matrix



Boundary Protection



Questions?



carly.logan@grayanalytics.com

https://www.linkedin.com/in/carlene-logan/

