Cyber Thursday:

CMMC: Correctly Scoping Your Environment

January 22| 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute

WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

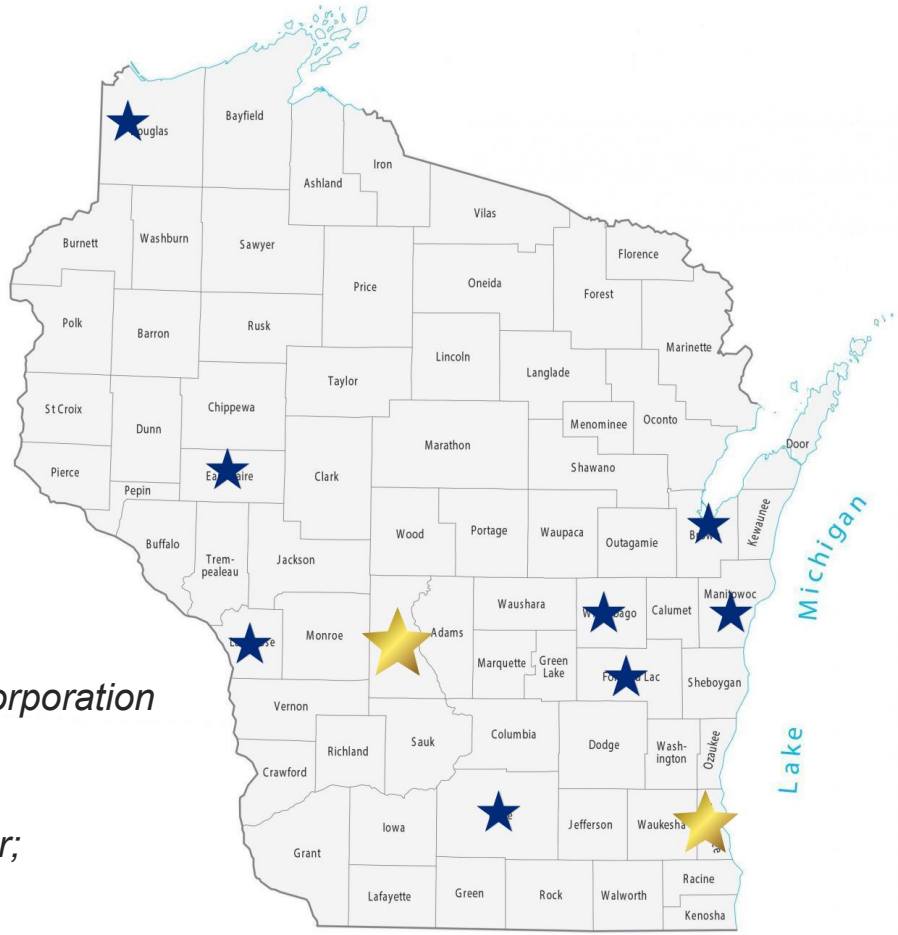
WPI provides services and training to all of Wisconsin's 72 counties

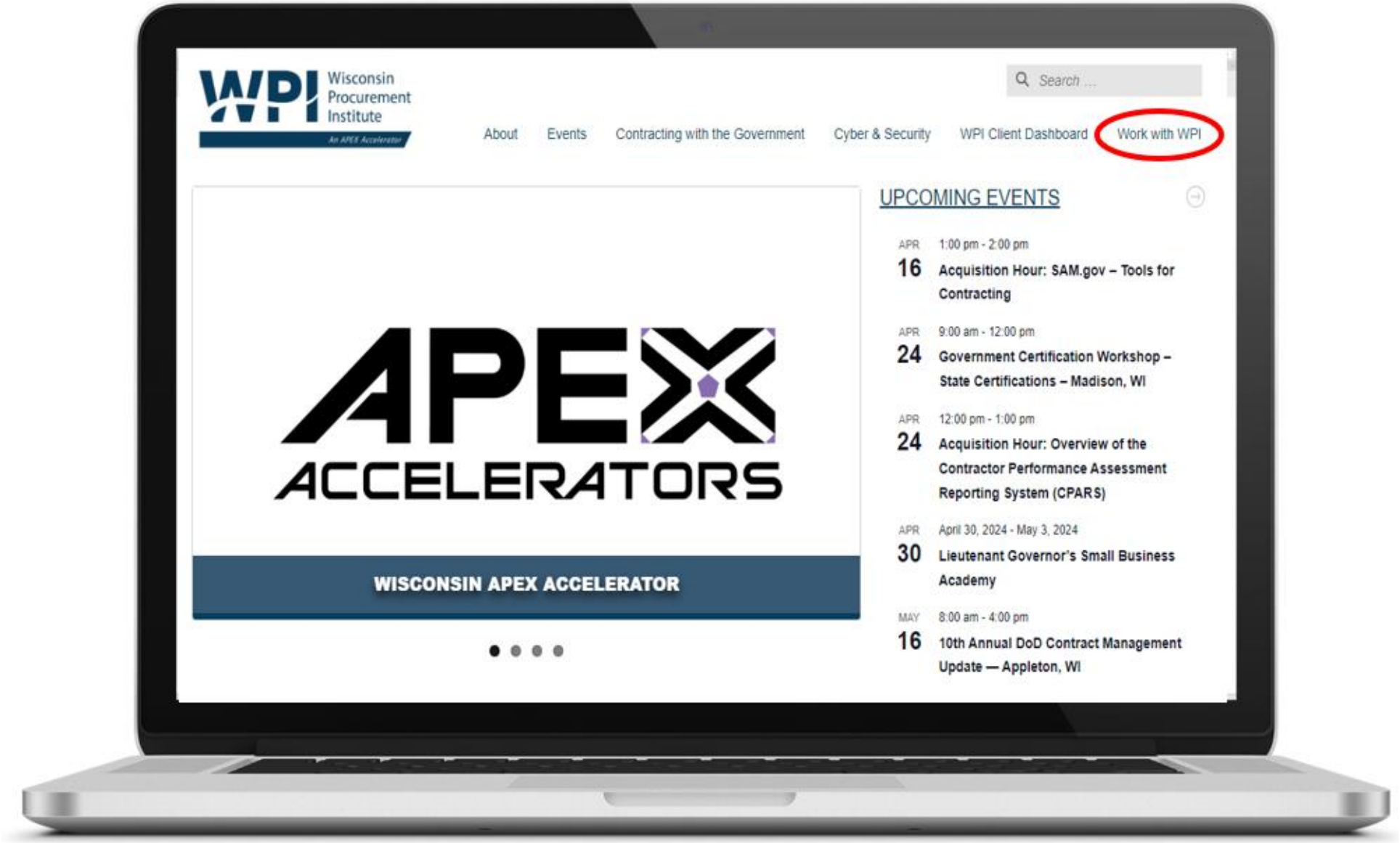
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more……

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*

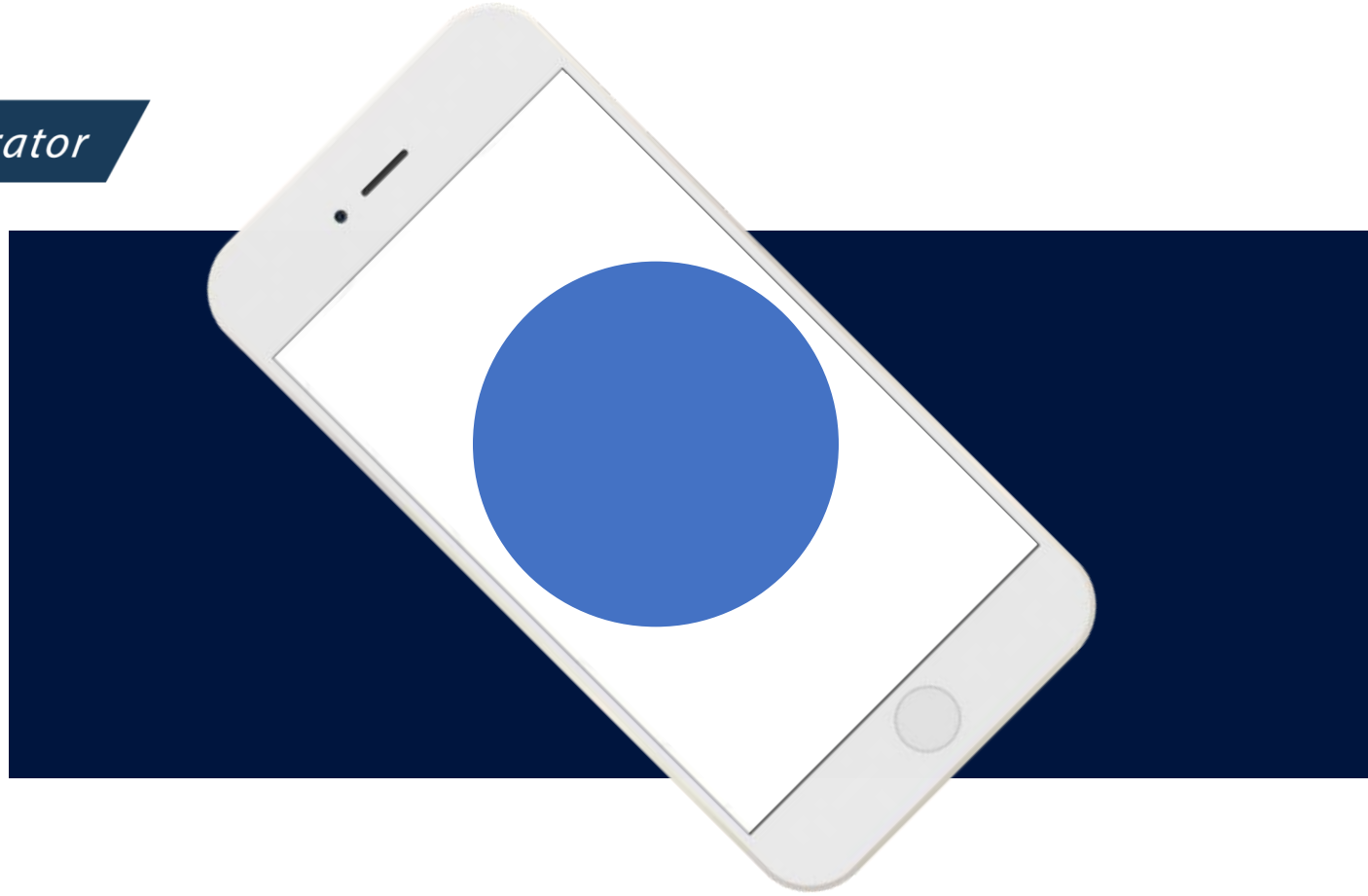



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Wisconsin Procurement Institute

An APEX Accelerator

Correctly Scoping your Environment



Cyber Thursday – January 22nd, 2026


LOCKHEED MARTIN
3103

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

DOCUMENT HEADINGS

Department of Defense
Office of the Secretary
32 CFR Part 170
[Docket ID: DoD-2023-OS-0063]
RIN 0790-AL49

1

CMMC Program

For verifying contractors have implemented security measures for FCI and CUI.

2

Tiered Implementation

Year 1: 135 Assessments
Year 2: 673 Assessments
Year 3: 2,252 Assessments
Year 4: 4,452 Assessments

3

Final Requirements

Level 1
Level 2 (Self)
Level 2 (C3PAO)
Level 3 (DIBCAC)

CMMC Levels and Requirements

TABLE 1—CMMC LEVEL AND ASSESSMENT REQUIREMENTS

CMMC status	Source & number of security reqts.	Assessment reqts.	Plan of action & milestones (POA&M) reqts.	Affirmation reqts.
Level 1 (Self) ...	• 15 required by FAR clause 52.204–21.	• Conducted by Organization Seeking Assessment (OSA) annually. • Results entered into SPRS (or its successor capability).	• Not permitted	• After each assessment. • Entered into SPRS.
Level 2 (Self) ...	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by OSA every 3 years ..... • Results entered into SPRS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 2 (C3PAO).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by C3PAO every 3 years ..... • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 3 (DIBCAC).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. • 24 selected from NIST SP 800–172 Feb2021, as detailed in table 1 to § 170.14(c)(4).	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment. • Conducted by Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every 3 years. • Results entered into CMMC eMASS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Level 2 (C3PAO) affirmation must also continue to be completed annually. • Entered into SPRS (or its successor capability).

Assessment Process

ASSESSMENT OBJECTIVES

Includes a determination statement related to the CUI security requirement that is the subject of the assessment.

Ex. 3.1.3 Control the flow of CUI in accordance with approved authorizations

ASSESSMENT METHODS

Define the nature and the extent of the assessor's actions. They include **examine**, **interview**, and **test**.

Ex. 3.1.3 Examine architectural solutions to control flow of system data.

ASSESSMENT OBJECTS

Identify specific items being assessed and can include specifications, mechanisms, activities, and individuals.

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

Assess each of the NIST SP 800-171 controls using the NIST SP 800-171A to ensure all audit points are covered.

ABOUT US ▾ ACCREDITATION ▾ RESOURCES ▾ CMMC ECOSYSTEM ▾ NEWS & EVENTS ▾ MARKETPLACE CAICO

www.cyberab.org

1

CMMC Assets

2

Separation Techniques

3

Artifacts

CMMC Assessment Scope
Level 2

Version 2.0 | December 2021

1. CMMC Assessment Scope (Level 2)
2. NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information
3. DoD Memo DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements

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

The Four In-Scope Asset Categories

- ❑ CUI Assets
- ❑ Security Protection Assets
- ❑ Contractor Risk Managed Assets
- ❑ Specialized Assets

Ok, but what is CUI?

- **Controlled Technical Information/Covered Defense Information** (Research Data, Engineering Data, Drawings, Specifications, Standards, Process Sheets, Manuals, Technical Reports, Technical Orders)

- **DoD Critical Infrastructure Security Information** (blueprints, information on the securing of explosive or hazardous chemicals, vulnerability assessments on DOD facilities or assets)

- **Anything Nuclear** (No, really. If it's regarding Nuclear Propulsion or Energy – it's like CUI at the bare minimum.)

CUI Assets

Assets that process, store, or transmit CUI.

- ❑ Laptops and Workstations
- ❑ Servers / Databases
- ❑ Cloud Services
- ❑ Mobile Devices, IoT Devices, Printers

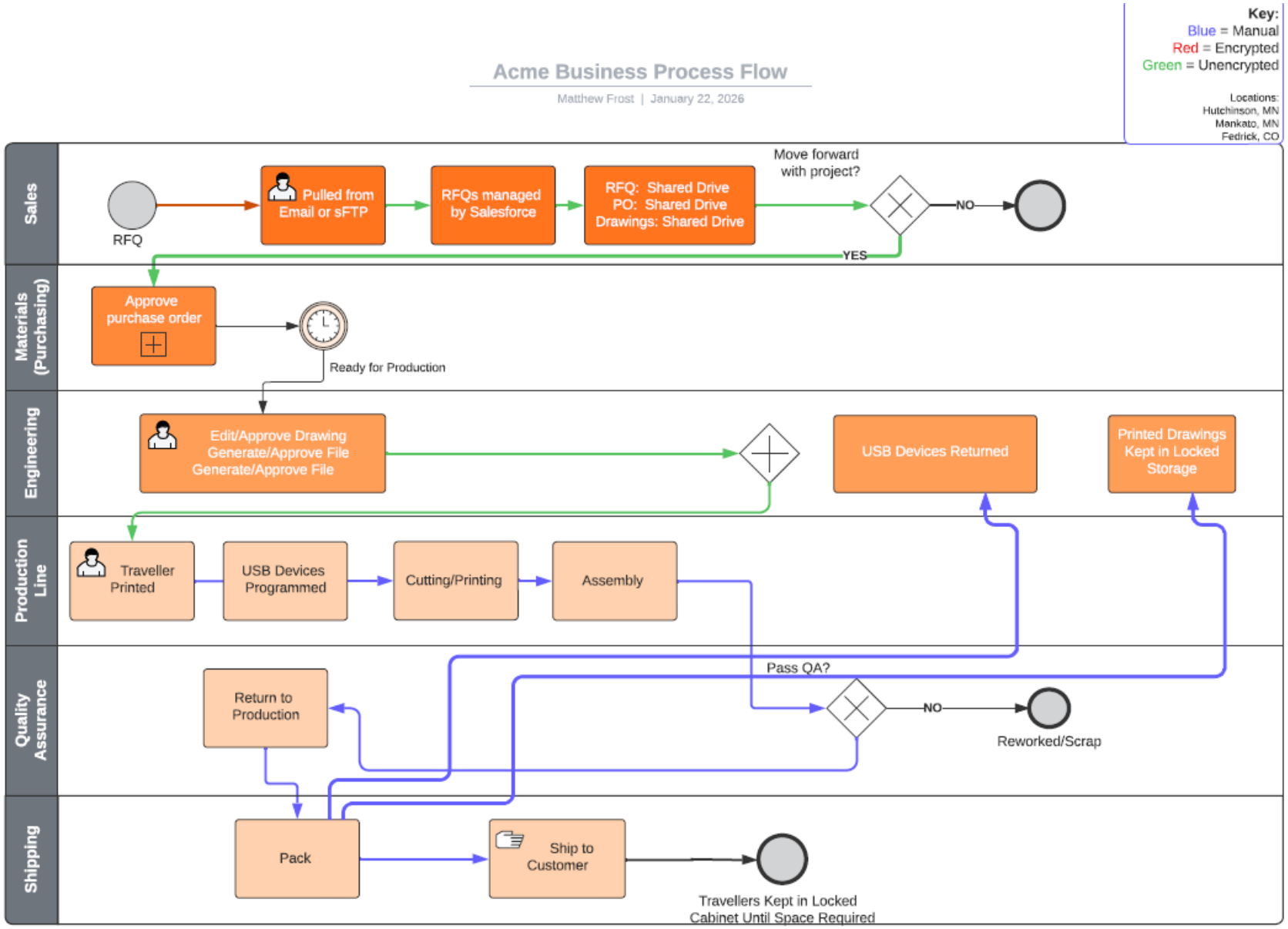
• **Process –** CUI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated, or printed).

• **Store –** CUI is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents).

• **Transmit –** CUI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).

Acme Business Process Flow

Matthew Frost | January 22, 2026



CUI Asset Requirements

What Must I Do?.

- ❑ Document in the asset inventory (hardware and software if necessary)
- ❑ Document in the System Security Plan
- ❑ Document in the Network Diagram of the CMMC Assessment Scope
- ❑ Prepare to be assessed against the 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.

- ❑ Firewalls
- ❑ SIEMs
- ❑ EDR, Vulnerability Scanners
- ❑ IAM tools like Active Directory/Azure

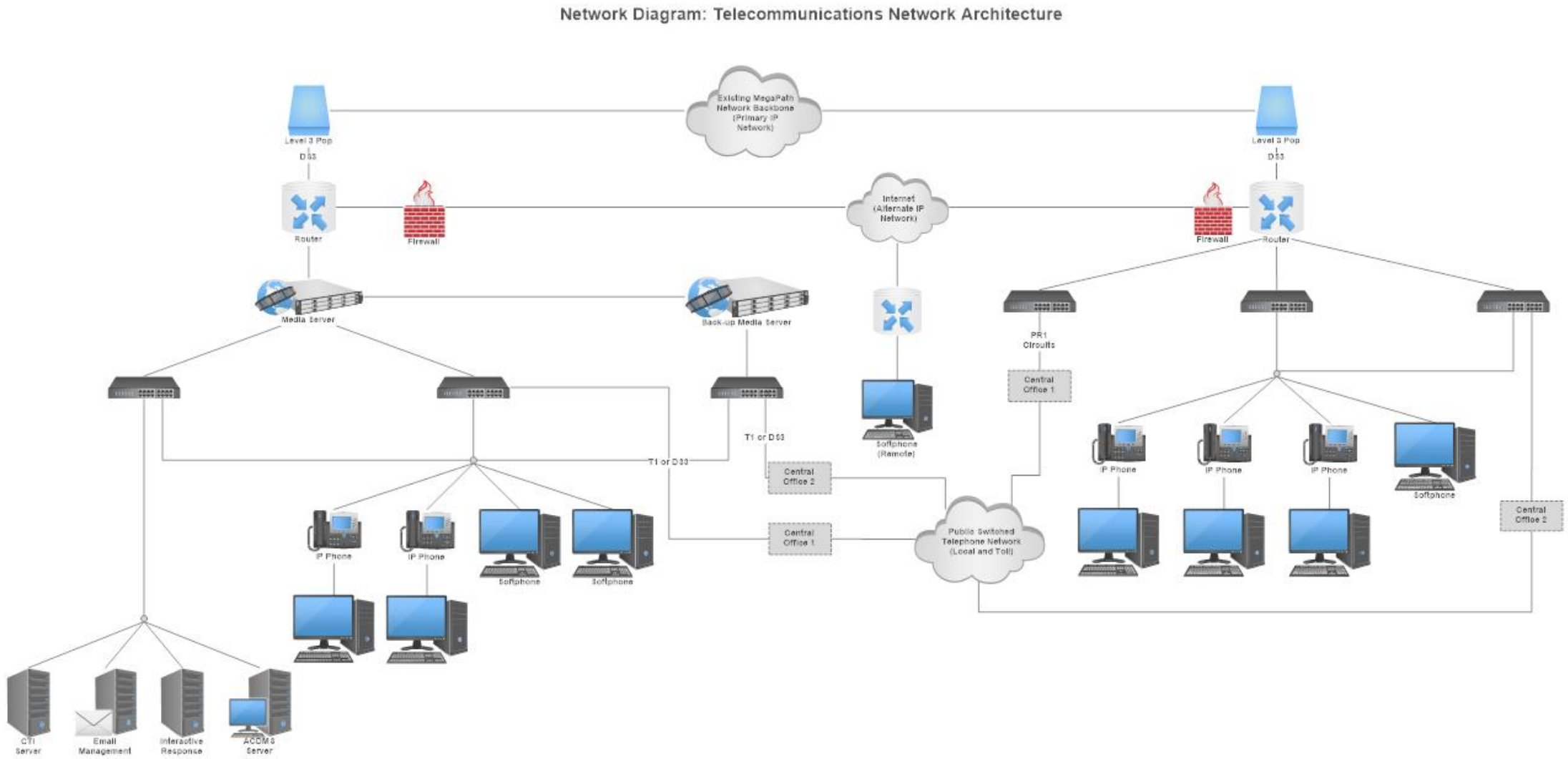
Security Protection Assets

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.

Table 2. Security Protection Asset Examples

Asset Type	Security Protection Asset Examples
People	• Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	• Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	• Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings

Security Protection Assets



SPA Requirements

What Must I Do?.

- ❑ Document in the asset inventory (hardware and software if necessary)
- ❑ Document in the System Security Plan
- ❑ Document in the Network Diagram of the CMMC Assessment Scope
- ❑ Prepare to be assessed against the CMMC Practices

Assessment Process

ASSESSMENT OBJECTIVES

Includes a determination statement related to the CUI security requirement that is the subject of the assessment.

Ex. 3.1.3 Control the flow of CUI in accordance with approved authorizations

ASSESSMENT METHODS

Define the nature and the extent of the assessor's actions. They include **examine**, **interview**, and **test**.

Ex. 3.1.3 Examine architectural solutions to control flow of system data.

ASSESSMENT OBJECTS

Identify specific items being assessed and can include specifications, mechanisms, activities, and individuals.

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

Assess each of the NIST SP 800-171 controls using the NIST SP 800-171A to ensure all audit points are covered.

Contractor Risk Managed Assets

CMMC Contractor Risk Managed Assets (CRMAs), also called Specialized Assets, are systems that might touch Controlled Unclassified Information (CUI) but aren't built to meet all NIST controls

- ❑ Operational Technology
- ❑ Test Equipment (QA)
- ❑ Shared IT Infrastructure
  (Commercial Network Segments)
- ❑ ERP Systems?

CRMA Requirements

What Must I Do?.

- ❑ Document in the asset inventory (hardware and software if necessary)
- ❑ Document in the System Security Plan (showing they are managed by security policies, procedures, and practices)
- ❑ Document in the Network Diagram of the CMMC Assessment Scope

Specialized Assets

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

Government Property is all property owned or leased by the government. Government property includes both government-furnished and contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property or software [Reference: Federal Acquisition Regulation (FAR) 52.245-1].

- **IoT or Industrial Internet of Things (IIoT)** are interconnected devices having physical or virtual representation in the digital world, sensing/actuation capability, and programmability features. They are uniquely identifiable and may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors [Reference: iot.ieee.org/definition; National Institute of Standards and Technology (NIST) 800-183].
- **OT**1 is used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems. OT may include programmable logic controllers (PLCs), computerized numerical control (CNC) devices, machine controllers, fabricators, assemblers, and machining.
- **Restricted Information Systems** can include systems [and associated Information Technology (IT) components comprising the system] that are configured based on government requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).
- **Test Equipment** can include hardware and/or associated IT components used in the testing of products, system components, and contract deliverables (e.g., oscilloscopes, spectrum analyzers, power meters, and special test equipment).

Specialized Assets Requirements

What Must I Do?.

- ❑ Document in the asset inventory (hardware and software if necessary)
- ❑ Document in the System Security Plan (showing they are managed by security policies, procedures, and practices)
- ❑ Document in the Network Diagram of the CMMC Assessment Scope

Not To Be Assessed But…

Must be documented in accordance with CA.L2 – 3.12.4

Can Still Be Spot Checked by Assessor

CA.L2-3.12.4

CA.L2-3.12.4 – SYSTEM SECURITY PLAN

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.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] a system security plan is developed;

[b] the system boundary is described and documented in the system security plan;

[c] the system environment of operation is described and documented in the system security plan;

[d] the security requirements identified and approved by the designated authority as non-applicable are identified;

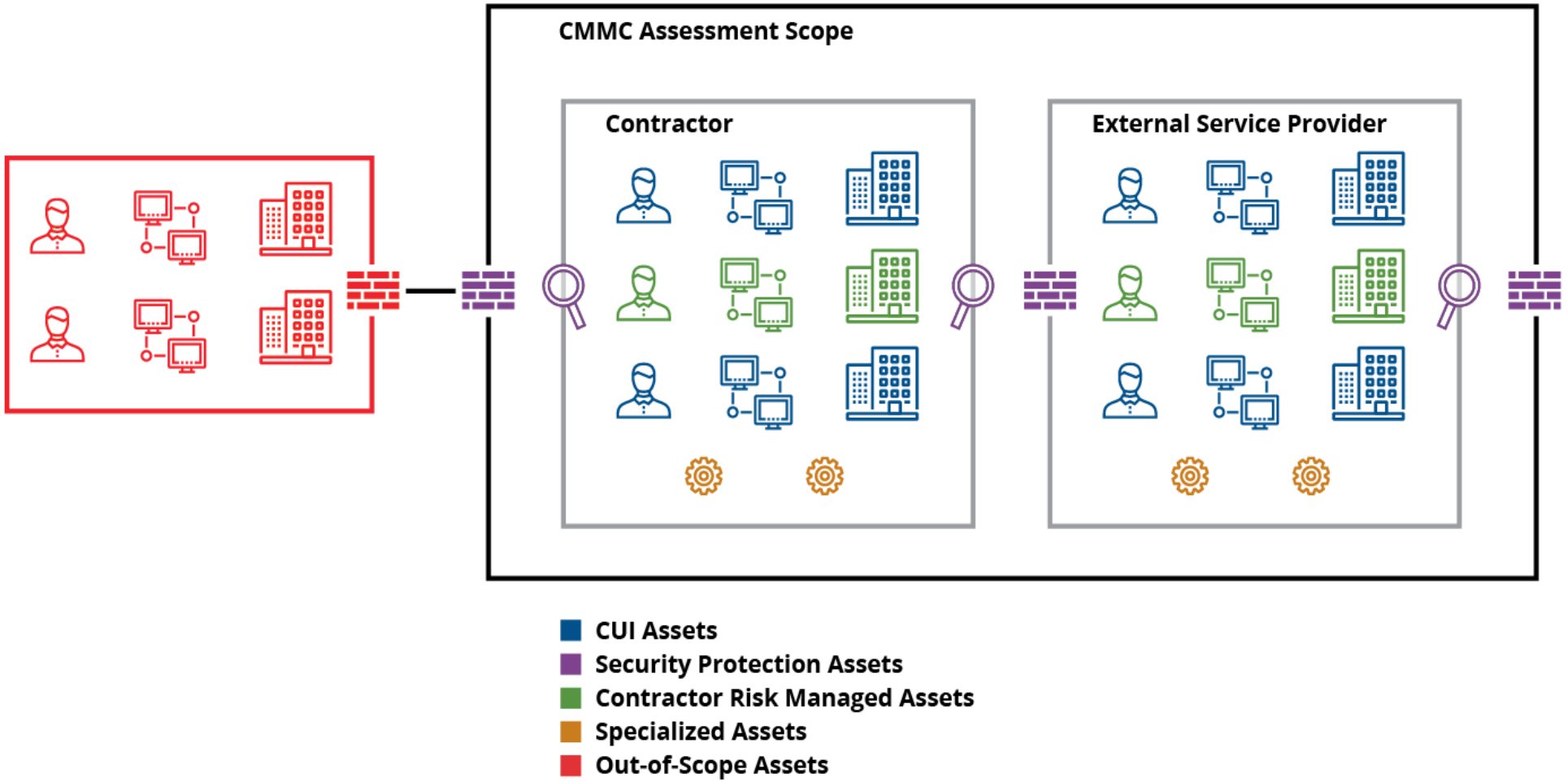
[e] the method of security requirement implementation is described and documented in the system security plan;

[f] the relationship with or connection to other systems is described and documented in the system security plan;

[g] the frequency to update the system security plan is defined; and

[h] system security plan is updated with the defined frequency.

Scoping Diagram



1

CMMC Assets

2

Separation Techniques

3

Artifacts

Separation Techniques

Logical Separation

occurs when an asset is physically (wired or wirelessly) connected to another asset or set of assets, but software configuration prevents data from flowing along the physical connection path. Examples of mechanisms that provide controlled logical access include:

- Firewalls
- Virtual Local Area Networks (VLANs).

Physical Separation

occurs when an asset is not physically (wired or wirelessly) connected to another asset or set of assets. Data may be transferred manually using human control (e.g., a USB drive). Examples of mechanisms that provide controlled physical access include:

- gates;
- locks;
- badge access; and
- guards.

1

CMMC Assets

2

Separation Techniques

3

Artifacts

Artifacts For Scoping

Scoping Diagram

- Identifies Scoping Boundaries between CUI Assets, SPAs, CRMAs, Specialized Assets, and Out Of Scope Asssets

Network Diagram

- Identifies Interconnectivity Between Hardware and Cloud Resources within Assessment Environment

Inventories (Hardware/Software)

- Identifies Hardware, Software, and Cloud Assets within Assessment Environment

Policy Documentation

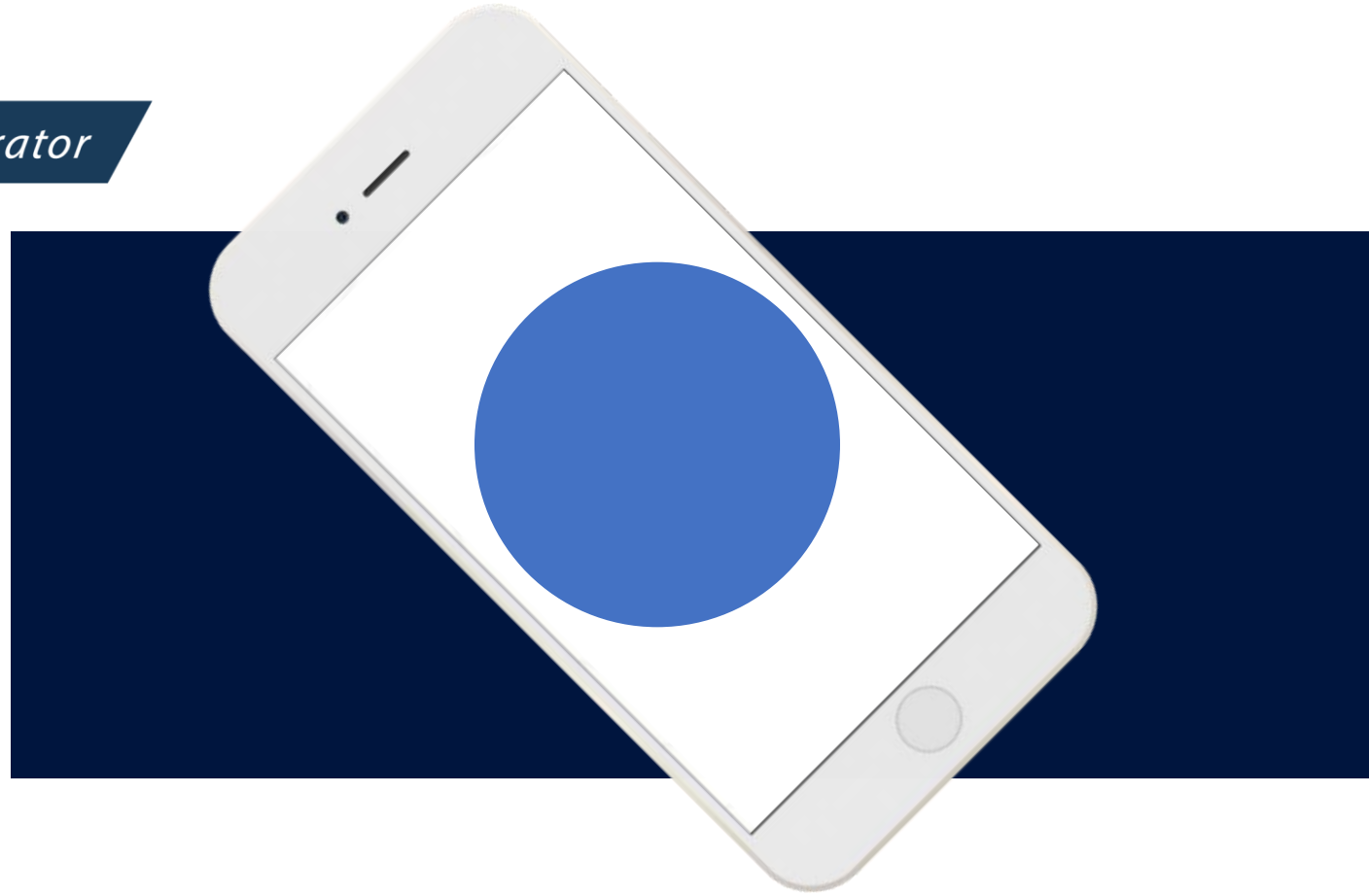
- States the Intention of the Architecture, Data Flow, and Restrictions on Usage within the Assessment Environment

Wisconsin Procurement Institute

An APEX Accelerator

Matthew Frost

mattf@wispro.org



APEX ACCELERATORS

Acquisition Hour

The Acquisition Hour webinar series covers a range of topics from market entry, sales growth, small business certifications, compliance, and more. Attendees receive 1 CPE credit for attending.

- **January 21**– The Basics of Cybersecurity for Any Small Business
- **February 11** – Is the GSA Schedule Right for Your Business?
- **February 18** – Overview of the Contractor Performance Assessment Reporting System (CPARS)

…More information and registrations at wispro.org/events

Cyber Thursday

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **January 22** – CMMC: Correctly Scoping Your Environment
- **February 26** – CMMC: Control Set Series: 3.1 Access Control
- **March 26** – CMMC: Control Set Series: 3.2 Awareness and Training
- **April 30** – CMMC: Control Set Series: 3.3 Audit and Accountability
- **May 28** – CMMC: Control Set Series: 3.4 Configuration Management

…More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

This webinar is eligible for

1 CPE credit

To receive a certificate of completion, contact apexaccelerator@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MatthewF@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226