



Cyber Friday
**Four Key Building Blocks to Use in Developing and
Implementing a Comprehensive System Security Plan**

October 7, 2022



Webinar Etiquette

PLEASE

- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
 - We will share the questions with our guest speaker who will respond to the group

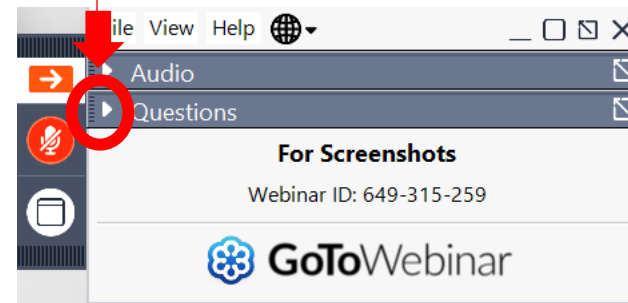
THANK YOU!

QUESTIONS?



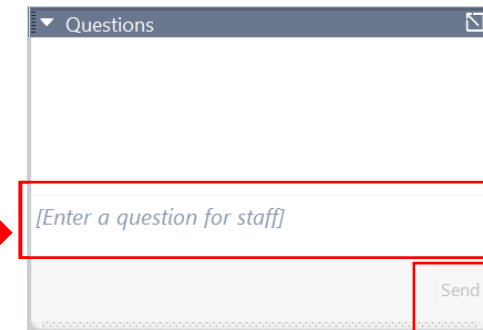
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

ABOUT WPI

Supporting the mission

WPI Wisconsin
Procurement
Institute

A Procurement Technical
Assistance Center (PTAC)

 Cyber Friday



Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING** – At our offices, at client’s facility or via telephone/GoToMeeting
- **SMALL GROUP TRAINING** – Workshops and webinars
- **CONFERENCES** to include one on one or roundtable sessions

Last year WPI provided training at over 100 events and provided service to over 1,200 companies



WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Department of Defense (DOD), WEDC and other funding sources.



Sign-up for our Newsletter

Stay up-to-date with the latest WPI news and events.

<https://www.wispro.org/newsletter-signup/>

WPI OFFICE LOCATIONS

▪ MILWAUKEE

- *Technology Innovation Center*

▪ MADISON

- *FEED Kitchens*
- *Dane County Latino Chamber of Commerce*
- *Wisconsin Manufacturing Extension Partnership (WMEP)*
- *Madison Area Technical College (MATC)*

▪ CAMP DOUGLAS

- *Juneau County Economic Development Corporation (JCEDC)*

▪ FOND DU LAC

- *Envision Greater Fond du Lac*

▪ GREEN BAY

- *NWTC Startup Hub*

▪ APPLETON

- *Fox Valley Technical College*

▪ OSHKOSH

- *Fox Valley Technical College*
- *Greater Oshkosh Economic Development Corporation*

▪ EAU CLAIRE

- *Western Dairyland*

▪ LADYSMITH

- *Indianhead Community Action Agency*

▪ RHINELANDER

- *Nicolet Area Technical College*

▪ ASHLAND

- *Ashland Area Development Corporation*

▪ FLORENCE

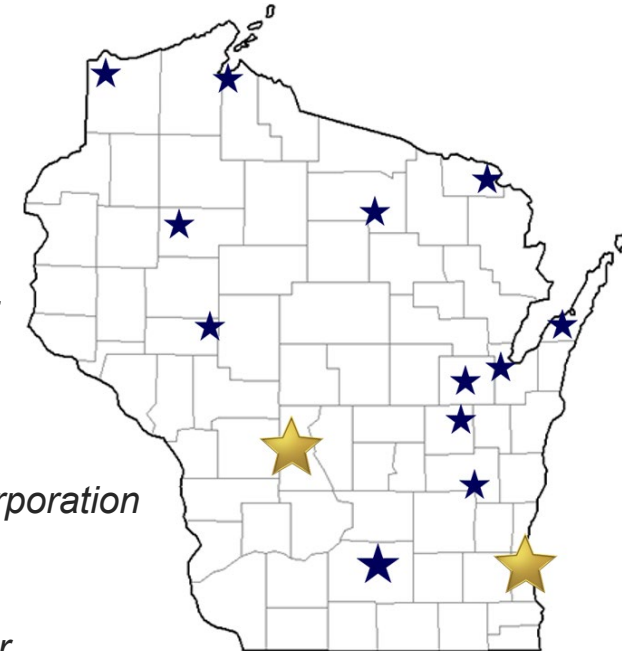
- *Florence County Economic Development*

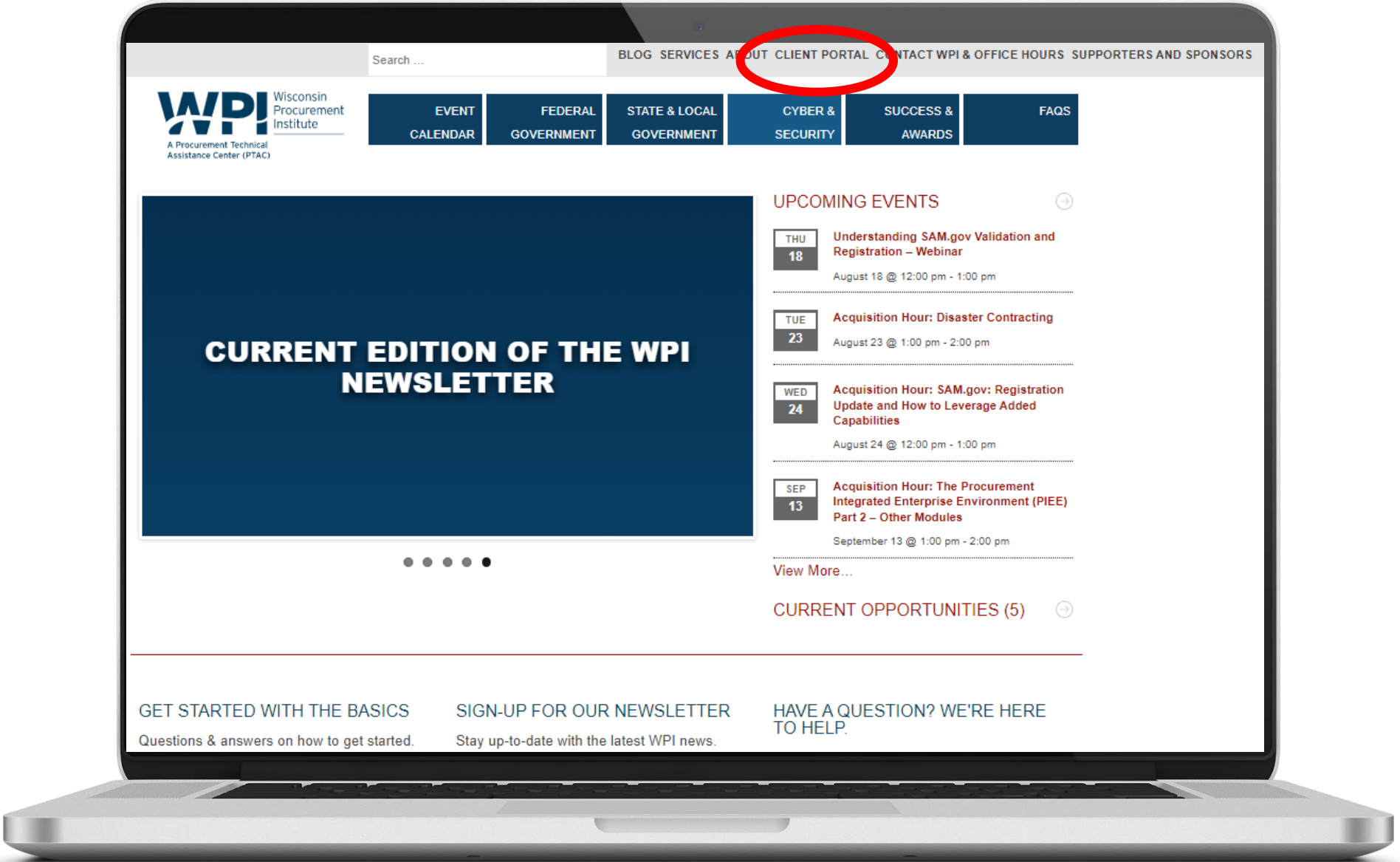
▪ DOOR COUNTY

- *NE WI Technical College*
- *Door County Economic Development Corporation*

▪ SUPERIOR

- *Small Business Dev Center; UW Superior*





Search ...

BLOG SERVICES ABOUT CLIENT PORTAL CONTACT WPI & OFFICE HOURS SUPPORTERS AND SPONSORS



- EVENT CALENDAR
- FEDERAL GOVERNMENT
- STATE & LOCAL GOVERNMENT
- CYBER & SECURITY
- SUCCESS & AWARDS
- FAQS

CURRENT EDITION OF THE WPI NEWSLETTER

UPCOMING EVENTS

- THU 18** Understanding SAM.gov Validation and Registration – Webinar
August 18 @ 12:00 pm - 1:00 pm
- TUE 23** Acquisition Hour: Disaster Contracting
August 23 @ 1:00 pm - 2:00 pm
- WED 24** Acquisition Hour: SAM.gov: Registration Update and How to Leverage Added Capabilities
August 24 @ 12:00 pm - 1:00 pm
- SEP 13** Acquisition Hour: The Procurement Integrated Enterprise Environment (PIEE) Part 2 – Other Modules
September 13 @ 1:00 pm - 2:00 pm

[View More...](#)

CURRENT OPPORTUNITIES (5)

[GET STARTED WITH THE BASICS](#)
Questions & answers on how to get started.

[SIGN-UP FOR OUR NEWSLETTER](#)
Stay up-to-date with the latest WPI news.

[HAVE A QUESTION? WE'RE HERE TO HELP.](#)

Four Key Building Blocks to Use in Developing and Implementing a Comprehensive System Security Plan

Marc Violante

Wisconsin Procurement Institute

October 7, 2022

Business Preparations - Description

- System Security Plans (SSP) are not solely a requirement created for NIST 800-171 and the DoD Basic Assessment. The system security plan is fundamental to all cyber security efforts. All companies should take time to develop one and manage it. Unfortunately, many DoD suppliers view the SSP as a byproduct of conducting the DoD Basic Assessment – essentially a checkmark generated document.
- A SSP should be one of the fundamental organizational documents that helps to guide the company in developing its IT infrastructure and establishing a firm foundation for protecting and securing all types of sensitive information by outlining company and customer driven cybersecurity requirements. This webinar will provide an overview of SSPs, the type of information used to develop SSPs, and four key considerations that should be incorporated into the plans.

Controlled Unclassified Information

- Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.
- DoD CUI Registry - <https://www.dodcui.mil/Home/DoD-CUI-Registry/>
- National CUI Registry - <https://www.archives.gov/cui>

SSPs – tunnel vision



SSP

- Nonfederal organizations describe, in a system security plan, how the security requirements are met or how organizations plan to meet the requirements and address known and anticipated threats. The system security plan describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems.

SSP - purpose

- The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.
- The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.
- The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Requirements (SSP) - overview

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Potential Impact - Confidentiality

Security Objective	LOW	MODERATE	HIGH
<p><i>Confidentiality</i> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

System Security Plan - topics

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

SSP use beyond DoD

- When requested, the system security plan (or extracts thereof) and the associated plans of action for any planned implementations or mitigations are submitted to the responsible federal agency/contracting office to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to a risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

“the manager accepts its associated risk”

- In order for the plans to adequately reflect the protection of the resources, a senior management official must authorize a system to operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

- Management authorization should be based on an assessment of management, operational, and technical controls. Since the system security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and the plan of actions and milestones. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur whenever there is a significant change in processing, but at least every three years.

System Security Plan – Focus on the “HOW”

APPLICABLE CUI SECURITY REQUIREMENTS

The system security plan is used to describe how the organization meets or plans to meet the CUI security requirements. Any security requirements that are deemed *non-applicable* by the organization (e.g., no wireless capability in the system or the system component processing, storing, or transmitting CUI), are documented as such in the system security plan. Once the system security plan is completed, a security assessment plan can be developed using the assessment procedures described in Chapter Three and tailoring those procedures as needed. An assessment procedure is developed for every CUI security requirement that is applicable to the system, system component, or the organization. Conversely, security requirements that are deemed non-applicable in the system security plan are *not* assessed.

Single State Security Solution

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the recommended security requirements contained in this publication are consistent with and are complementary to the standards and guidelines used by federal agencies to protect CUI.

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

It's all about CUI!

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

North Atlantic Treaty Organization (NATO)	<ul style="list-style-type: none"> • NATO Restricted • NATO Unclassified
Nuclear	<ul style="list-style-type: none"> • General Nuclear • Nuclear Recommendation Material • Nuclear Security-Related Information • Safeguards Information • Unclassified Controlled Nuclear Information - Energy
Patent	<ul style="list-style-type: none"> • Patent Applications • Inventions • Secrecy Orders
Privacy	<ul style="list-style-type: none"> • Contract Use • Death Records • General Privacy • Genetic Information • Health Information • Inspector General Protected • Military Personnel Records • Personnel Records • Student Records
Procurement and Acquisition	<ul style="list-style-type: none"> • General Procurement and Acquisition • Small Business Research and Technology • Source Selection
Proprietary Business Information	<ul style="list-style-type: none"> • Entity Registration Information • General Proprietary Business Information • Ocean Common Carrier and Marine Terminal Operator Agreements • Ocean Common Carrier Service Contracts • Proprietary Manufacturer • Proprietary Postal
Provisional	<ul style="list-style-type: none"> • Homeland Security Agreement Information • Homeland Security Enforcement Information • Information Systems Vulnerability Information - Homeland • International Agreement Information - Homeland • Operations Security Information • Personnel Security Information • Physical Security - Homeland • Privacy Information • Sensitive Personally Identifiable Information

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

Four Key Building Blocks of the SSP



Minimum Security Requirements

- Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the federal government and the success of the resulting security measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.
- ***Specifications for Minimum Security Requirements Access Control (AC)***: Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

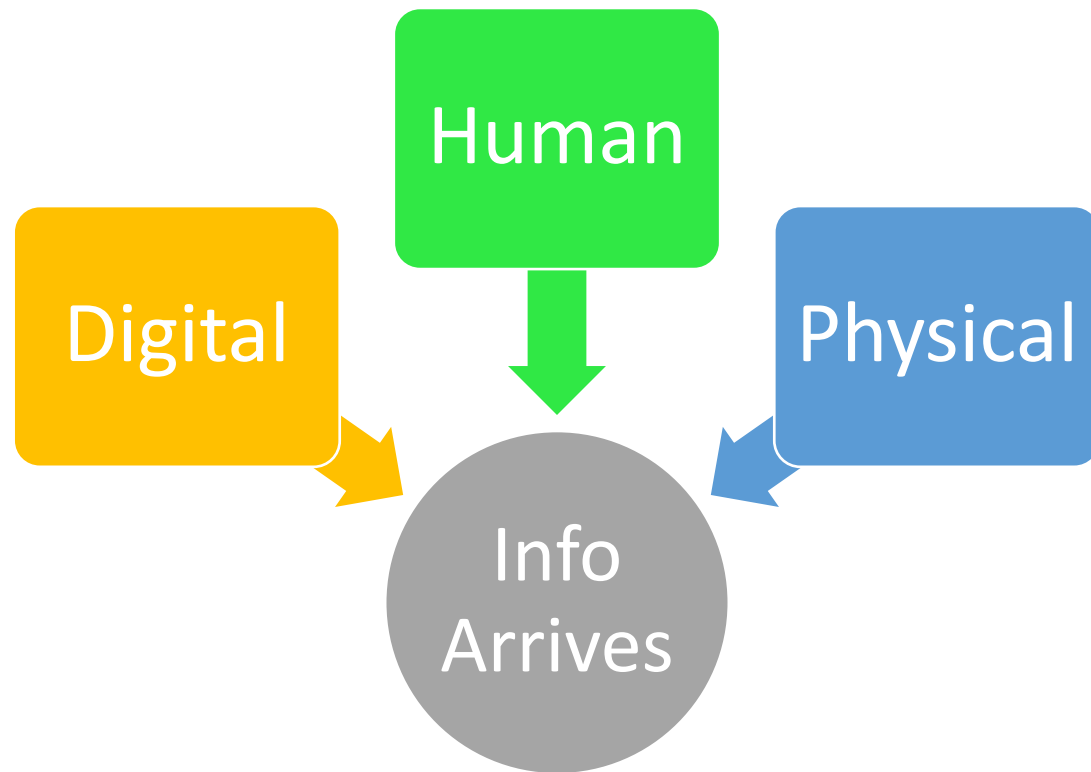
Requirements for the SSP

- The system security plan describes:
 - the system boundary*;
 - operational environment;
 - how security requirements are implemented; and
 - the relationships with or connections to other systems.

Information Security

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Flows - internal



- What pathways are used?
- Who uses?
- How is it protected?
- Where is it stored?
- How is it tracked?
- How is dissemination tracked?
- How is the process audited?
- How is information destroyed?

General Security Framework

- Awareness of security requirements
 - Information
 - Business framework – current
- Awareness of the presence of and type of information
 - CUI | Export Controlled (JCP/ITAR/NOFORN)
- Ability to know where the information is at a point in time
 - Who has access to the information
 - Who has accessed/used/using the information

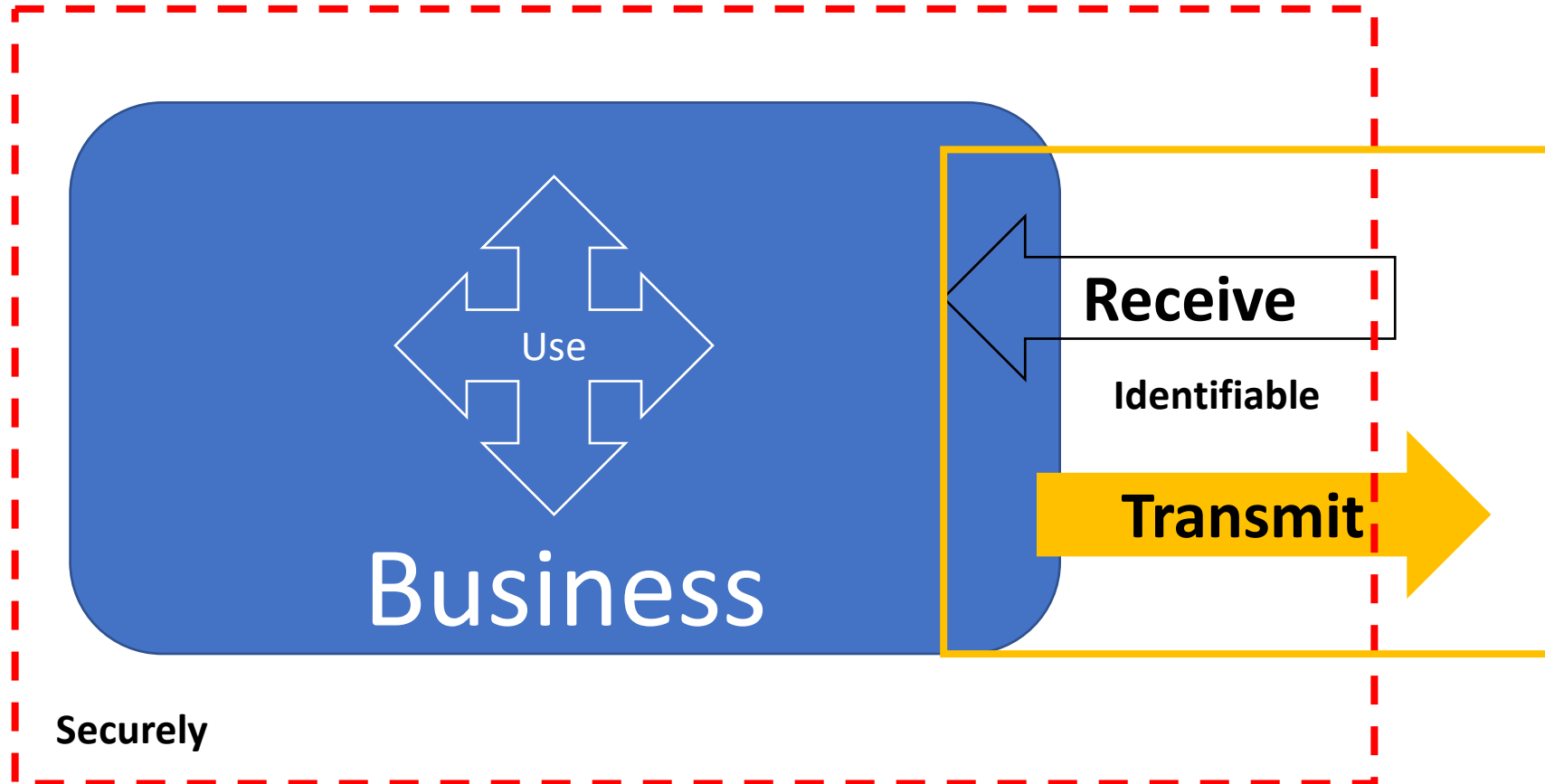
Access Lists
Logs

Policies formal appointment – Data Custodian, Procedures (check in/out), logs

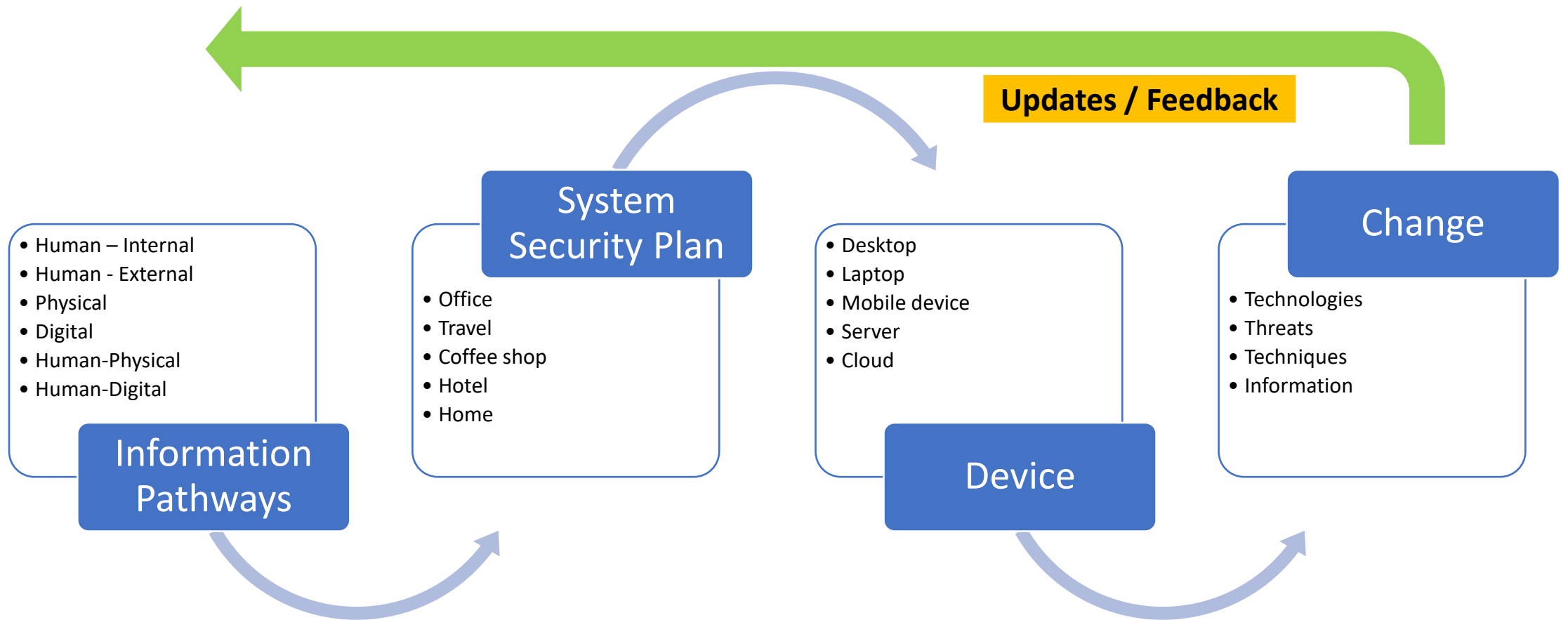
System Boundary/Authorization Boundary

1. ***“The process of uniquely assigning information resources to an information system defines the security boundary for that system.”**
NIST 800-18 pg 9
 1. Information resources consist of information and related resources, such as personnel, equipment, funds, and information technology.
2. All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Information Flows



Dynamic/Evolving Environment



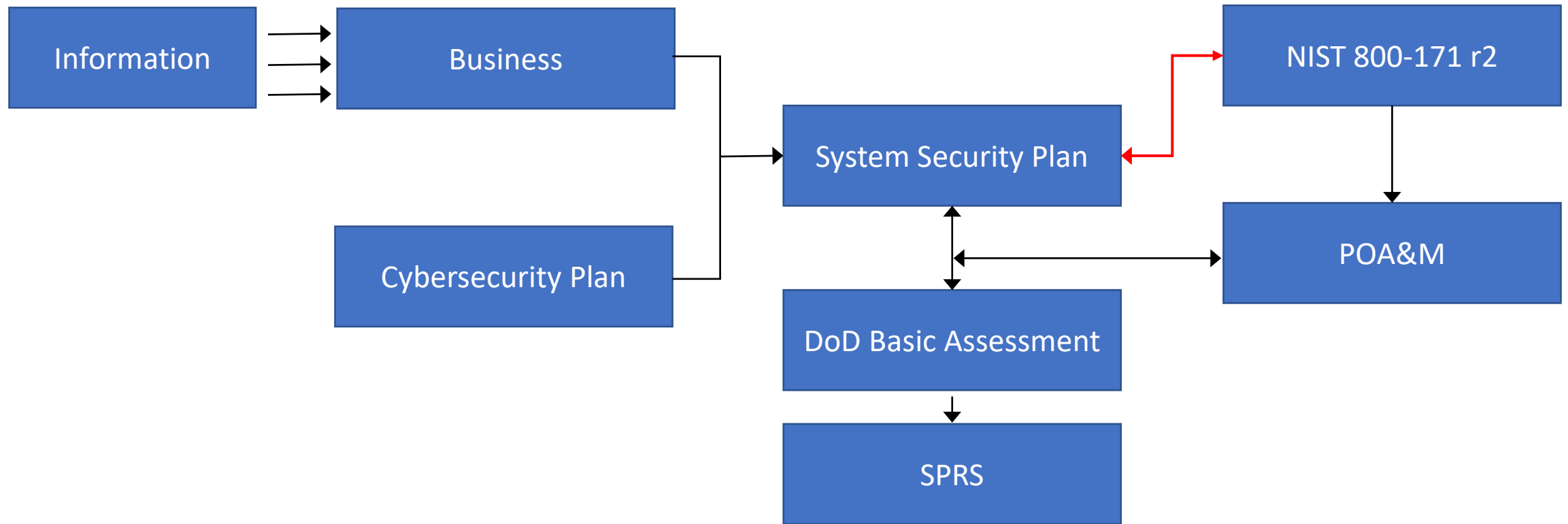
Boundary Protection

- we recommend employing boundary protection specific to the high-value system to ensure that it is sufficiently isolated, including from the rest of the enterprise. In addition, all of the traffic entering and exiting the high-value system environment should be inspected.
- Required inbound and outbound traffic for high-value systems should be understood and documented at the IP address, port, and protocol level of detail. This information can be used to ensure that system network communications are denied by default and allowed by exception, in accordance with the security design principle of [Least Privilege](#).

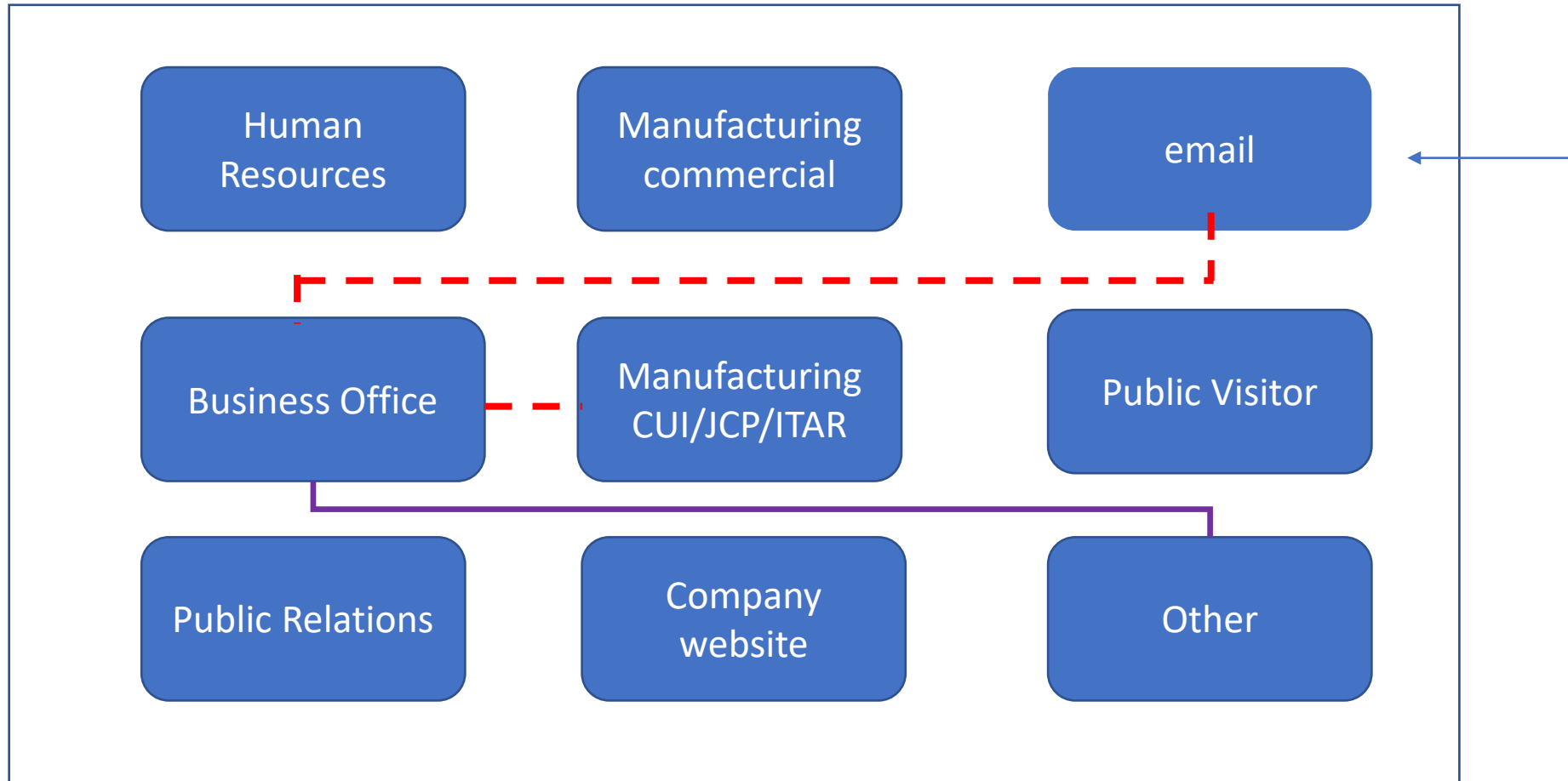
System Boundary - identification

- To properly identify an information system's boundary, you must identify not only where the data is stored, but also where system data flows, as well as critical dependencies.

Major Cybersecurity Elements & Flow



System Interconnections



System Environment

Provide a brief (one to three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc. Typically, operational environments are as follows:

- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, to small businesses and small branch offices of a company.
- **Managed or Enterprise** are typically large agency systems with defined, organized suites of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.
- **Custom** environments contain systems in which the functionality and degree of security do not fit the other environments. Two typical Custom environments are **Specialized Security-Limited Functionality and Legacy**:

Boundary Protection

- [Boundary protection](#) is the "monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication." Protection is achieved through the use of gateways, routers, firewalls, guards, and encrypted tunnels.

Asset (Organizational Asset)

- Anything that has value to an organization, including, but not limited to: another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards) [NISTIR 7693, NISTIR 7694].
Understanding assets is critical to identifying the CMMC Self-Assessment Scope; for more information, see CMMC Self-Assessment Scope – Level 1.

Security Protection Asset Examples

Asset Type	Security Protection Asset Examples
People	<ul style="list-style-type: none">• Consultants who provide cybersecurity service• Managed service provider personnel who perform system maintenance• Enterprise network administrators
Technology	<ul style="list-style-type: none">• Cloud-based security solutions• Hosted Virtual Private Network (VPN) services• SIEM solutions
Facility	<ul style="list-style-type: none">• Co-located data centers• Security Operations Centers (SOCs)• Contractor office buildings

Contractor Risk Managed Assets

Contractor Risk Managed Assets are part of the CMMC Assessment Scope. These assets are managed using the contractor's risk-based information security policy, procedures, and practices and are not assessed against CMMC practices.

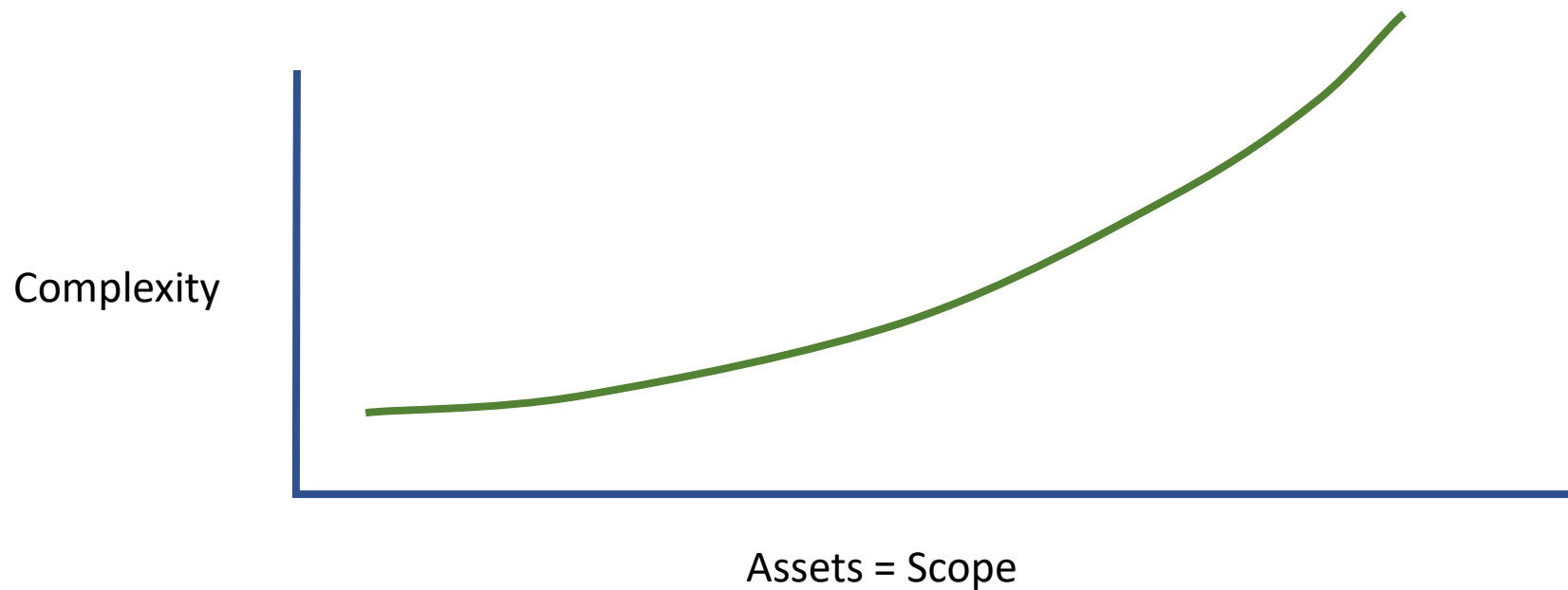
At a minimum, the contractor is required to:

- document these assets in asset inventory;
- document these assets in the SSP to show they are managed using the contractor's risk-based security policies, procedures, and practices; and
- provide a network diagram of the assessment scope (to include these assets) to facilitate scoping discussions during the pre-assessment.

Inventory | SSP | Network Diagram

Information Protection Difficulty

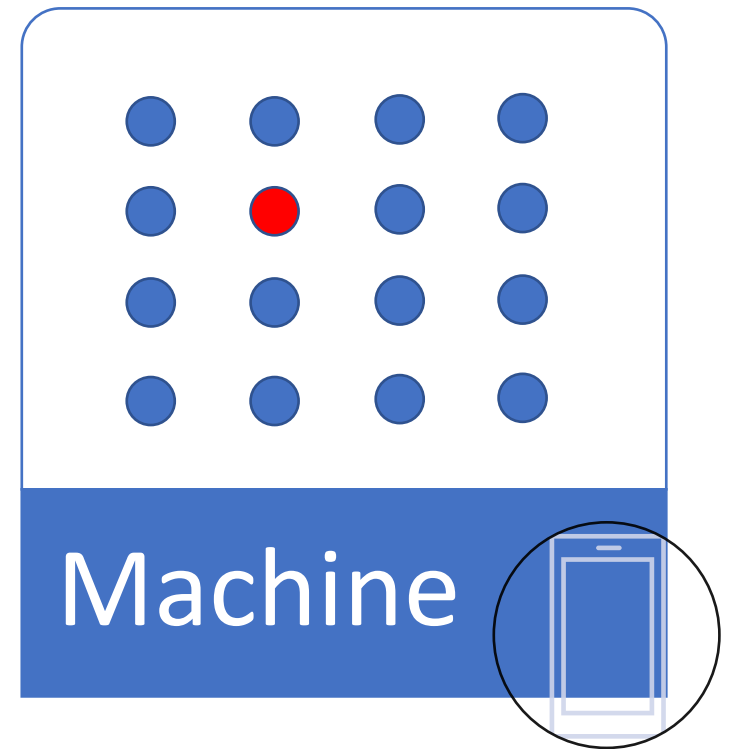
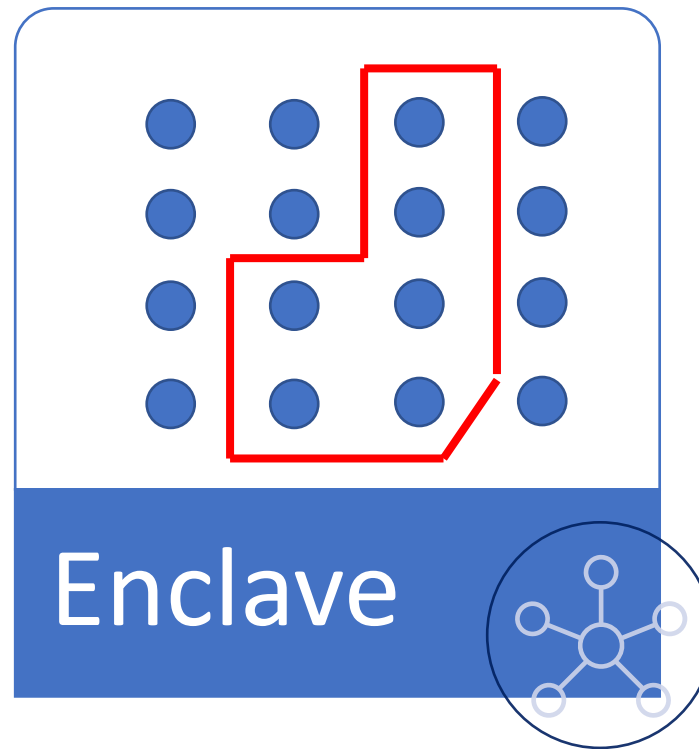
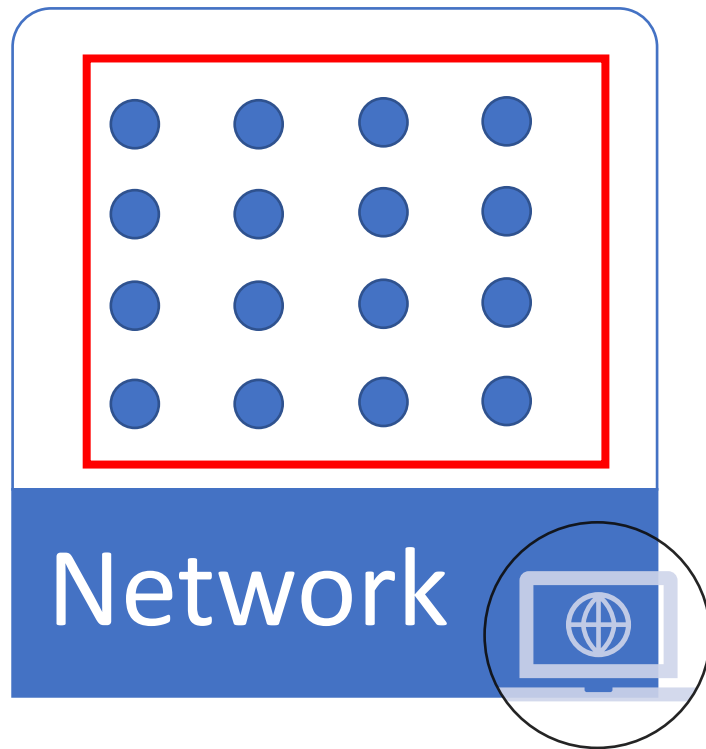
Assets = Scope = CMMC Assessment Complexity



Operational Environment

- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, to small businesses and small branch offices of a company.
- **Managed or Enterprise** are typically large agency systems with defined, organized suites of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.
- **Custom** environments contain systems in which the functionality and degree of security do not fit the other environments. Two typical Custom environments are **Specialized Security-Limited Functionality and Legacy:**

Determine needs to be secured



How security requirements are implemented

- Formal requirements apply to systems involving CUI
- Scope – key concept related to managing CUI
 - Who receives
 - Who uses
 - How stored
- It's not strictly about having a plan or a list
- It's more about – how – why – who – when - what

Security requirement implementation

- It's more about -
 - “how the access list was developed”
 - “who was selected and why”
 - “what level of access is given; what systems are involved; what access is required,

Goal / Requirement Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Access List

- Who is on the list?
- Why were they selected?
- What was the process used?
- What would happen if two or three individuals were taken off the list?
- Are they qualified?
- Have they been trained?

Questions

- Does the company have only one access list?
- Are all machines on the same network?
- How is information segregated?
- How are copies controlled?
- How does the Data Custodian manage in-bound/outbound information?

For example

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
	ASSESSMENT OBJECTIVE <i>Determine if:</i>	
	3.1.1[a]	<i>authorized users are identified.</i>
	3.1.1[b]	<i>processes acting on behalf of authorized users are identified.</i>
	3.1.1[c]	<i>devices (and other systems) authorized to connect to the system are identified.</i>
	3.1.1[d]	<i>system access is limited to authorized users.</i>
	3.1.1[e]	<i>system access is limited to processes acting on behalf of authorized users.</i>
	3.1.1[f]	<i>system access is limited to authorized devices (including other systems).</i>

Ongoing System Security Plan Maintenance

- Change in information system owner;
- Change in information security representative;
- Change in system architecture;
- Change in system status;
- Additions/deletions of system interconnections;
- Change in system scope;
- Change in authorizing official; and
- Change in certification and accreditation status

CUI – Basic

- **CUI Basic** is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

CUI - Specified

- **CUI Specified** is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

Generalized Format – Information System

The generalized format for expressing the security category, SC, of an information system is:

SC information system = $\{(\mathbf{confidentiality}, \mathit{impact}), (\mathbf{integrity}, \mathit{impact}), (\mathbf{availability}, \mathit{impact})\}$,

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

★ Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

Definitions (DFARS 252.204-7012)

- “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- “Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
- *Information* means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

NIST 800-171 r2 Appendix E

- Organizations that are interested in or are required to comply with the recommendations in this publication are strongly advised to review the complete listing of controls in the moderate baseline in [Appendix E](#) to ensure that their individual security plans and control deployments provide the necessary and sufficient protection to address the cyber and kinetic threats to organizational missions and business operations.

Tailoring Action Symbols

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

TABLE E-12: TAILORING ACTIONS FOR PLANNING CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PL-1	Security Planning Policy and Procedures	NFO
PL-2	System Security Plan	CUI
PL-2(3)	<i>SYSTEM SECURITY PLAN PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</i>	NFO
PL-4	Rules of Behavior	NFO
PL-4(1)	<i>RULES OF BEHAVIOR SOCIAL MEDIA AND NETWORKING RESTRICTIONS</i>	NFO
PL-8	Information Security Architecture	NFO

The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization’s comprehensive security program

CYBER FRIDAY LIVE WEBINAR SERIES

- October 7, 2022

Four Key Building Blocks to Use in Developing and Implementing a Comprehensive System Security Plan

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute

- October 21, 2022

Vetting and Creating Agreements with Subcontractors and 3rd Party Service Providers

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute

- November 4, 2022

Developing and Implementing Essential Security Policies, Practices, and Procedures

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute

PRESENTED BY



**TECHNOLOGY
INNOVATION CENTER**
— at RESEARCH PARK



ACQUISITION HOUR LIVE WEBINAR SERIES

- October 18
Marketing Your Business to the Government
- October 18
Certifications for Woman Owned Businesses
- October 19
Certifications for Minority Owned Businesses
- October 19
Preparing for One-on-One Buyer Meetings
- November 1
Preparing for One-on-One Buyer Meetings
- November 15
Certifications for Veteran Owned Businesses
- November 29
The HUBZone Program – Certification Benefits and Regulations
- January 10
The SBA 8(a) Program and Small Disadvantaged Business (SDB) Program

Save the date



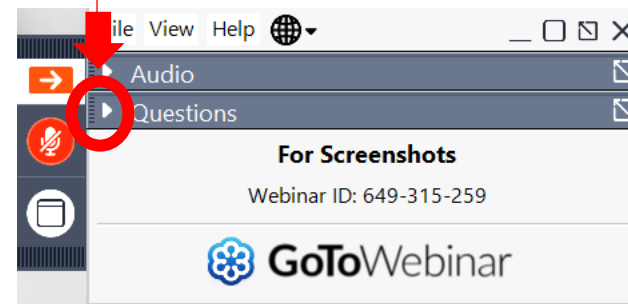
MarketplaceWisconsin.com

QUESTIONS?



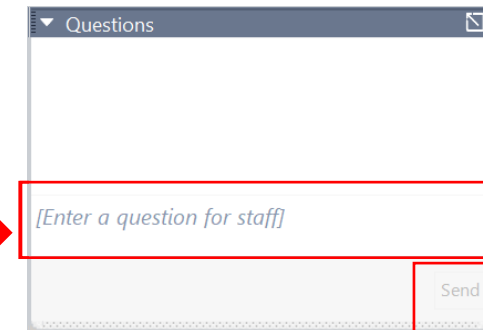
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



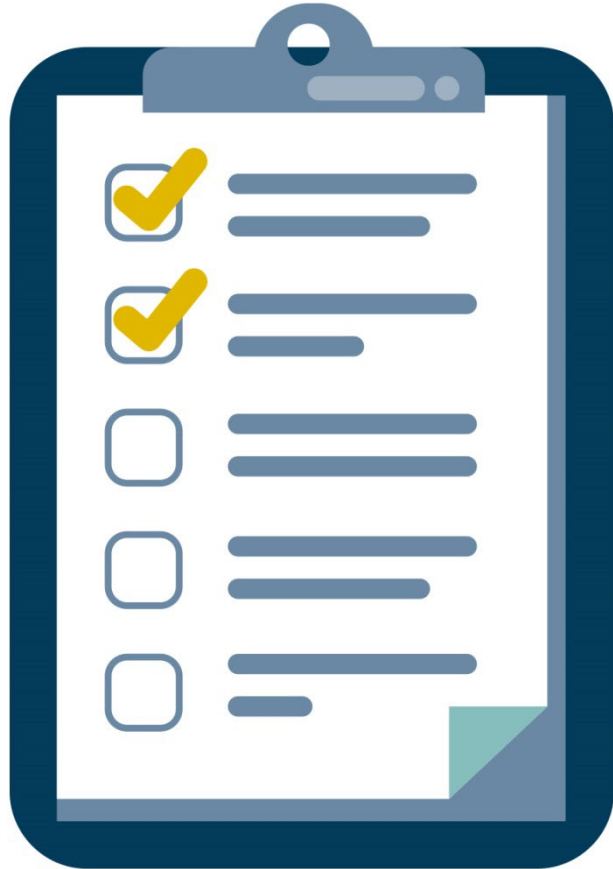
USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

SURVEY



CONTINUING PROFESSIONAL EDUCATION



This webinar is eligible for 1 CPE credit.
For a certificate of this credit, please contact:

Caroline Boettcher

carolineb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Marc Violante

Wisconsin Procurement Institute (WPI)

marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226