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

Marc Violante

Wisconsin Procurement Institute

October 7, 2022

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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 conduction 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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION, page 9

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.

NIST Special Publication 800-18 Revision 1; Guide for Developing Security Plans for Federal Information Systems; page vii

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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION - Abstract

Potential Impact - Confidentiality

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

FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems

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

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION; page 7

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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION, page 10

“the manger 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.

NIST Special Publication 800-18 Revision 1; Guide for Developing Security Plans for Federal Information Systems; page vii

- 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.

NIST Special Publication 800-18 Revision 1; Guide for Developing Security Plans for Federal Information Systems; page vii

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.

NIST SP 800-171A ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION; page 7

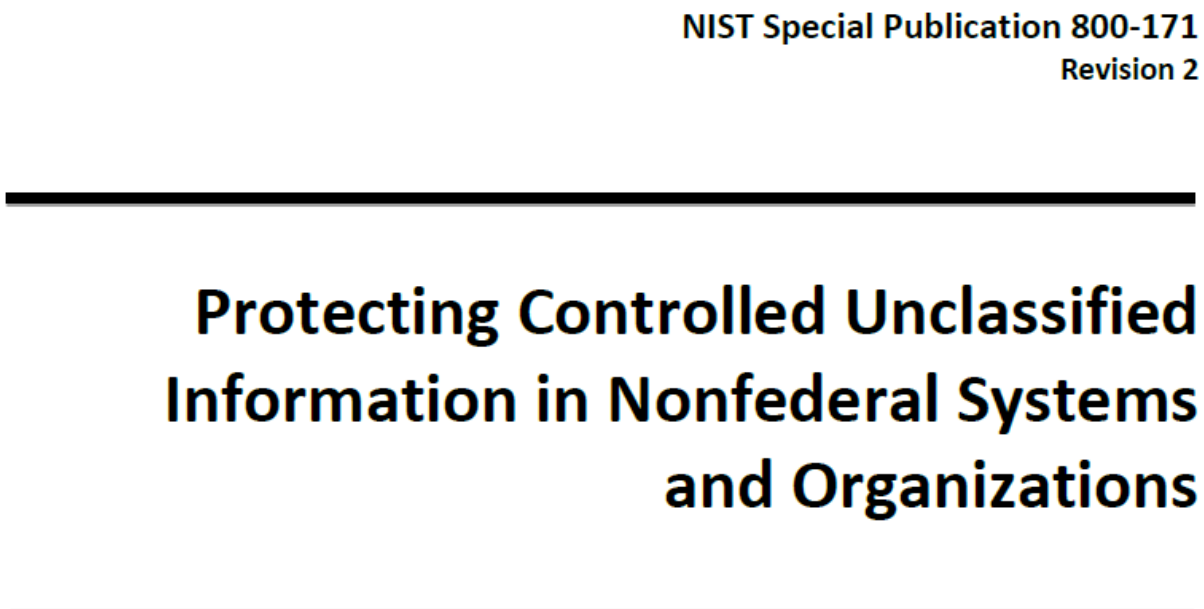
Single State Security Solution

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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION; page 5 and 6

CUI – NIST 800-171 r2 - Applicability



It’s all about CUI!

CUI – Categories; partial

North Atlantic Treaty Organization (NATO)	• NATO Restricted • NATO Unclassified
Nuclear	• General Nuclear • Nuclear Recommendation Material • Nuclear Security-Related Information • Safeguards Information • Unclassified Controlled Nuclear Information - Energy
Patent	• Patent Applications • Inventions • Secrecy Orders
Privacy	• Contract Use • Death Records • General Privacy • Genetic Information • Health Information • Inspector General Protected • Military Personnel Records • Personnel Records • Student Records
Procurement and Acquisition	• General Procurement and Acquisition • Small Business Research and Technology • Source Selection
Proprietary Business Information	• 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	• 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.

FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems; page 2

Requirements for the SSP

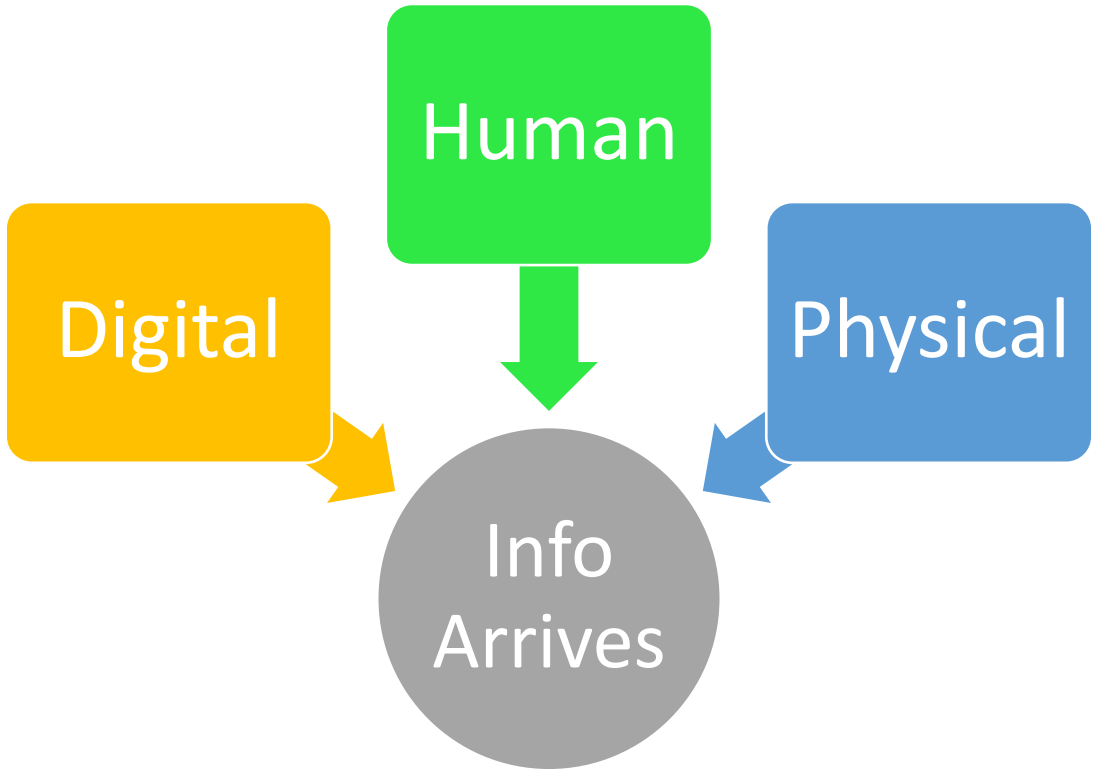
- The system security plan describes:
  - the system boundary*;
  - operational environment;
  - how security requirements are implemented; and
  - the relationships with or connections to other systems.

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.

44 U.S.C., Sec. 3542

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

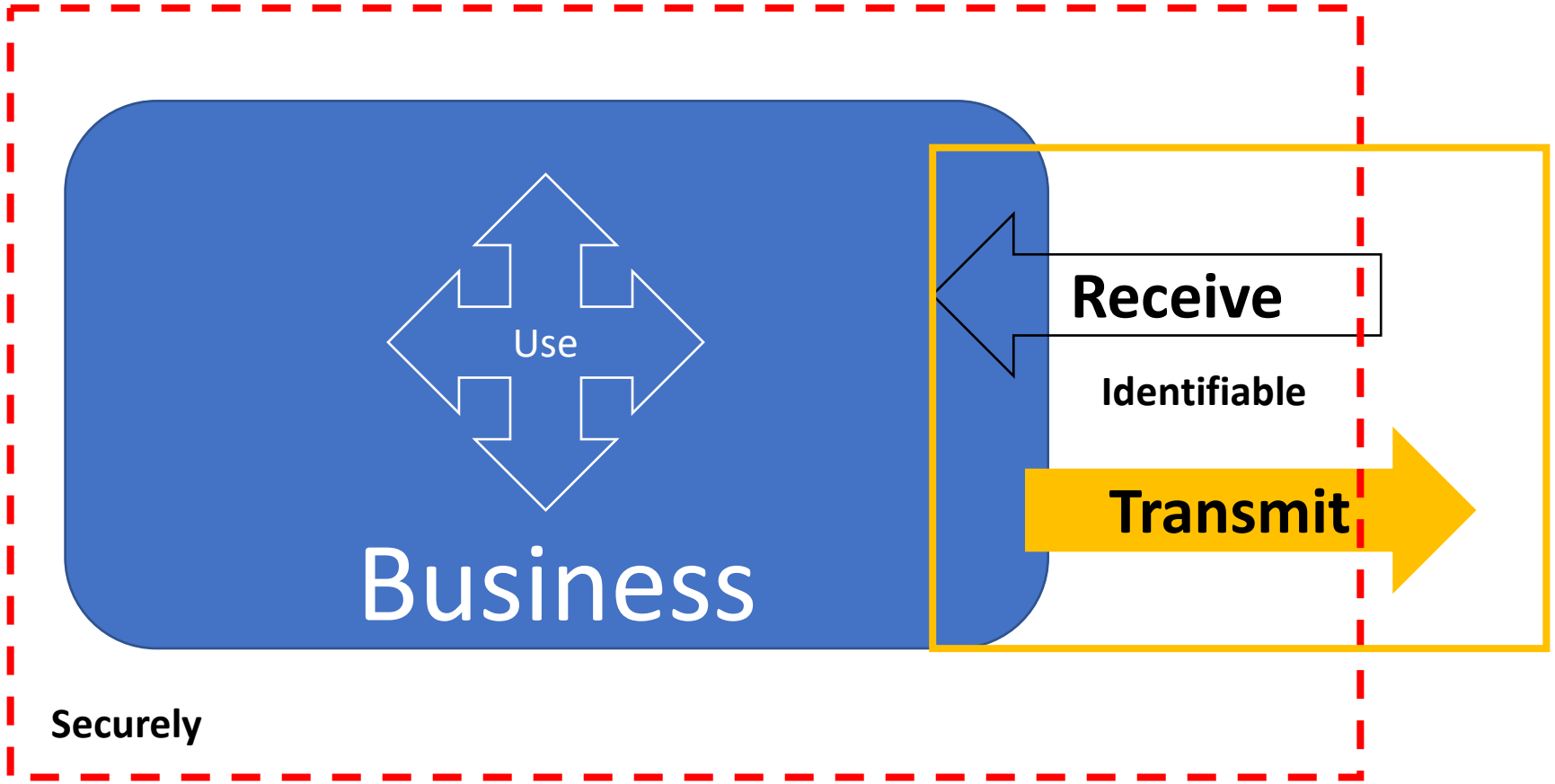
Policies formal appointment – Data Custodian, Procedures (check in/out), logs

System Boundary/Authorization Boundary

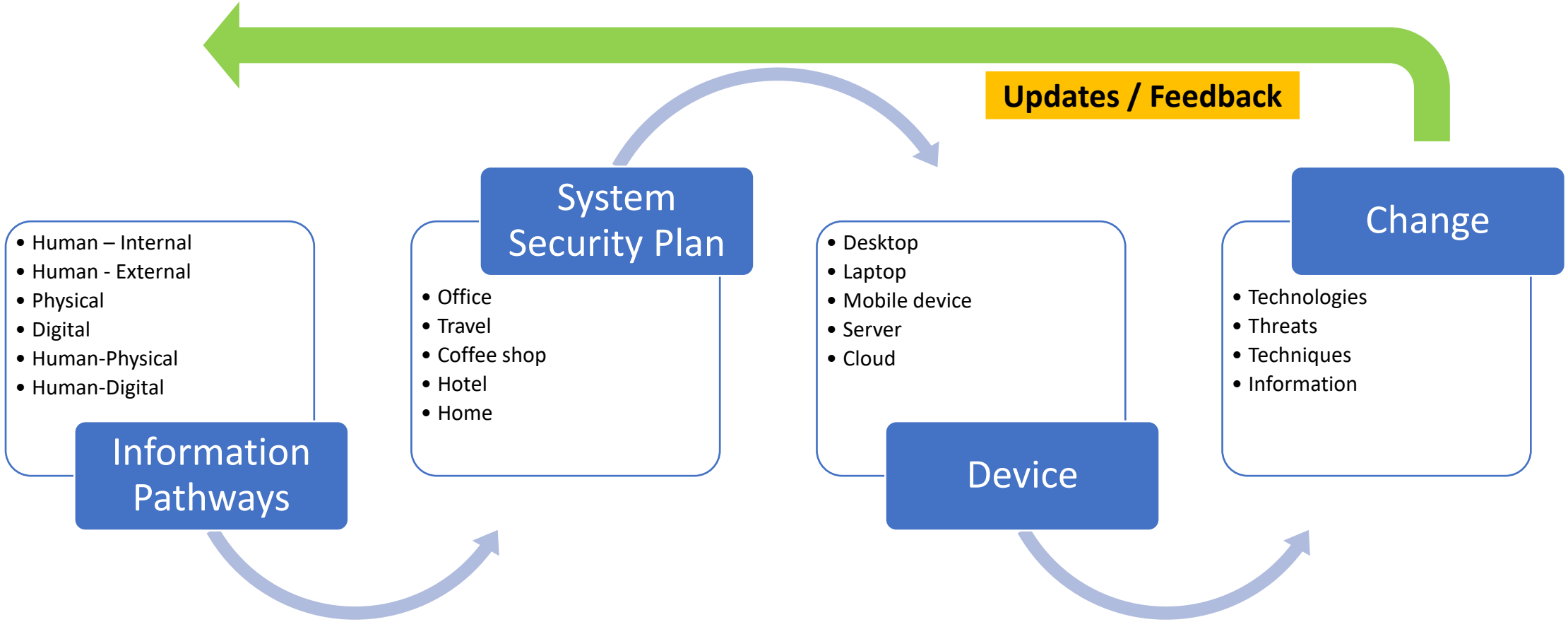
1. *“The process of uniquely assigning information resources to an information system defines the security boundary for that system.” NIST 800-18 pg 9
    1. Information resources consist of information and related resources, such as personnel, equipment, funds, and information technology.
2. All components 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.

https://csrc.nist.gov/glossary/term/authorization_boundary & NIST 800-18 pg 9

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.

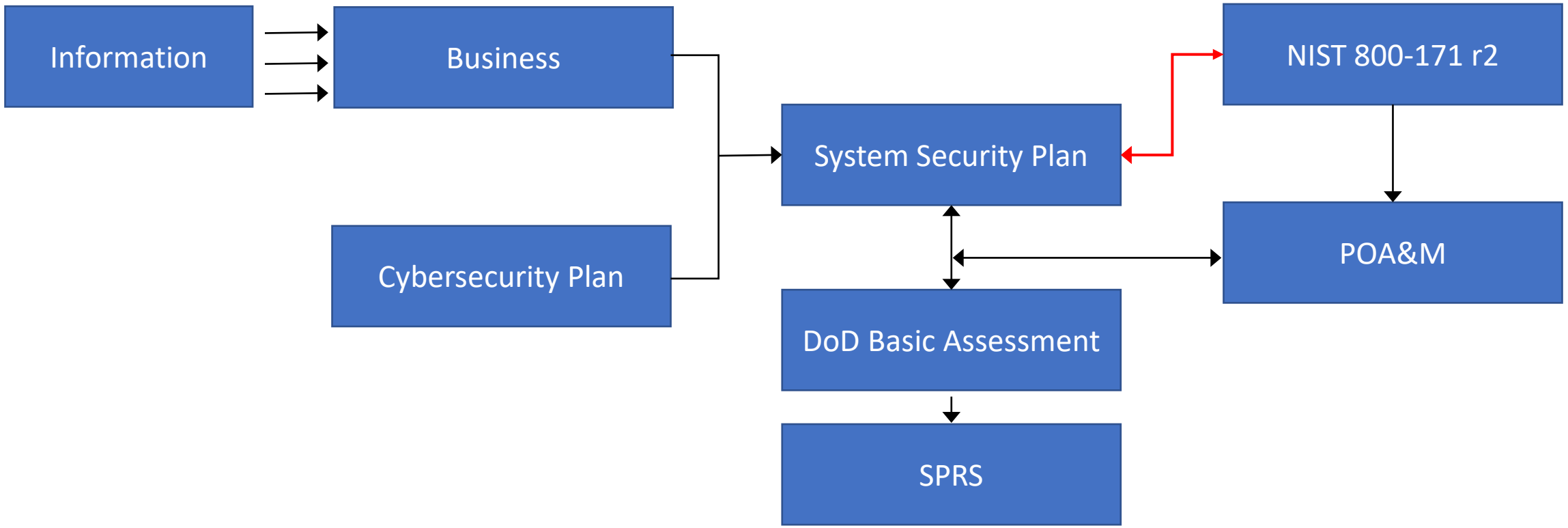
https://insights.sei.cmu.edu/blog/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection/

System Boundary - identification

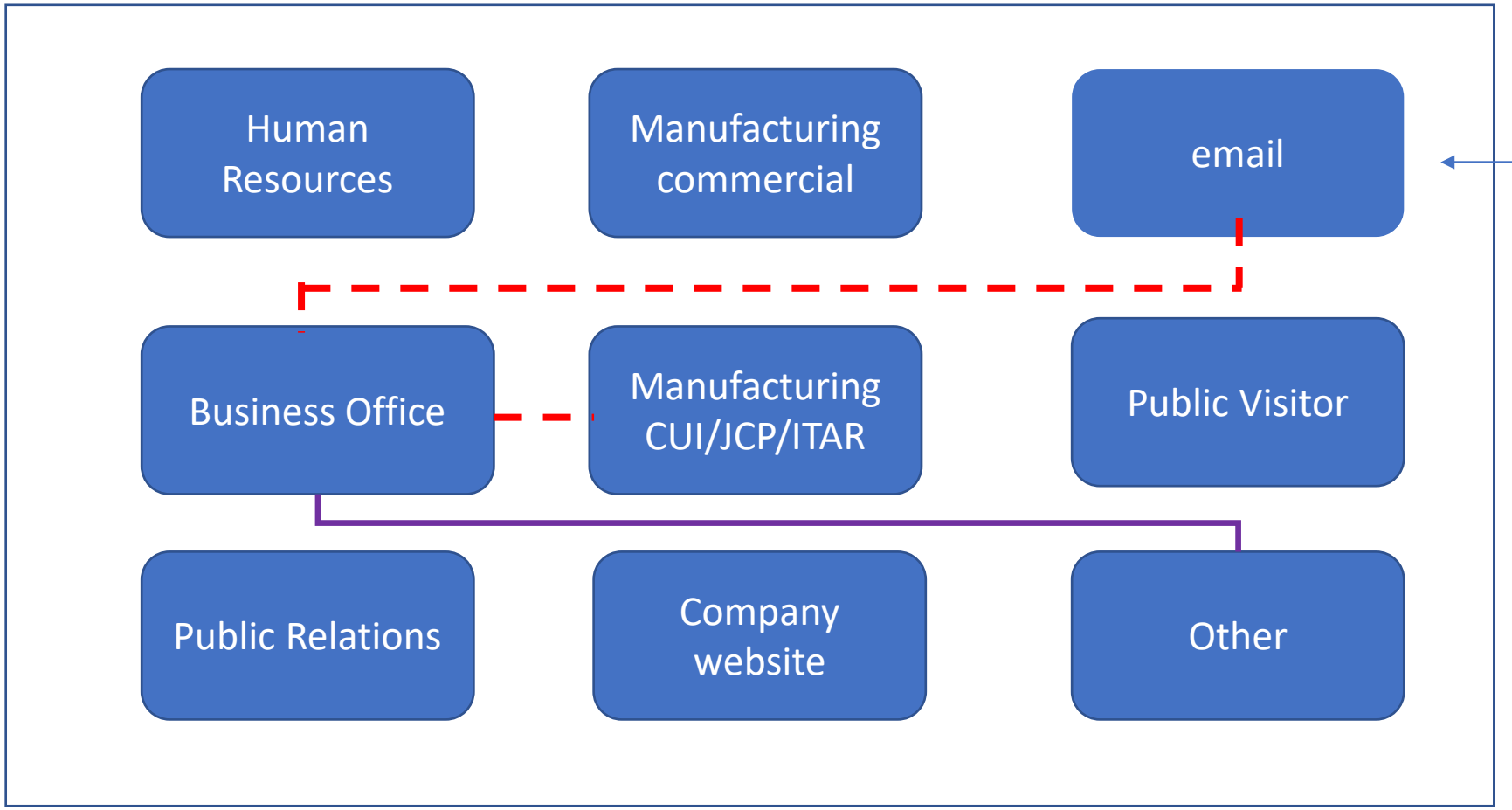
- To properly identify an information system's boundary, you must identify not only where the data is stored, but also where system data flows, as well as critical dependencies.

https://insights.sei.cmu.edu/blog/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection/

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**:

NIST SP 800-18 r1 - Guide for Developing Security Plans for Federal Information Systems, page 22

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.

https://insights.sei.cmu.edu/blog/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection/

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	• 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

CMMC Assessment Scope – Level 2 | Version 2.0; page 4

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:

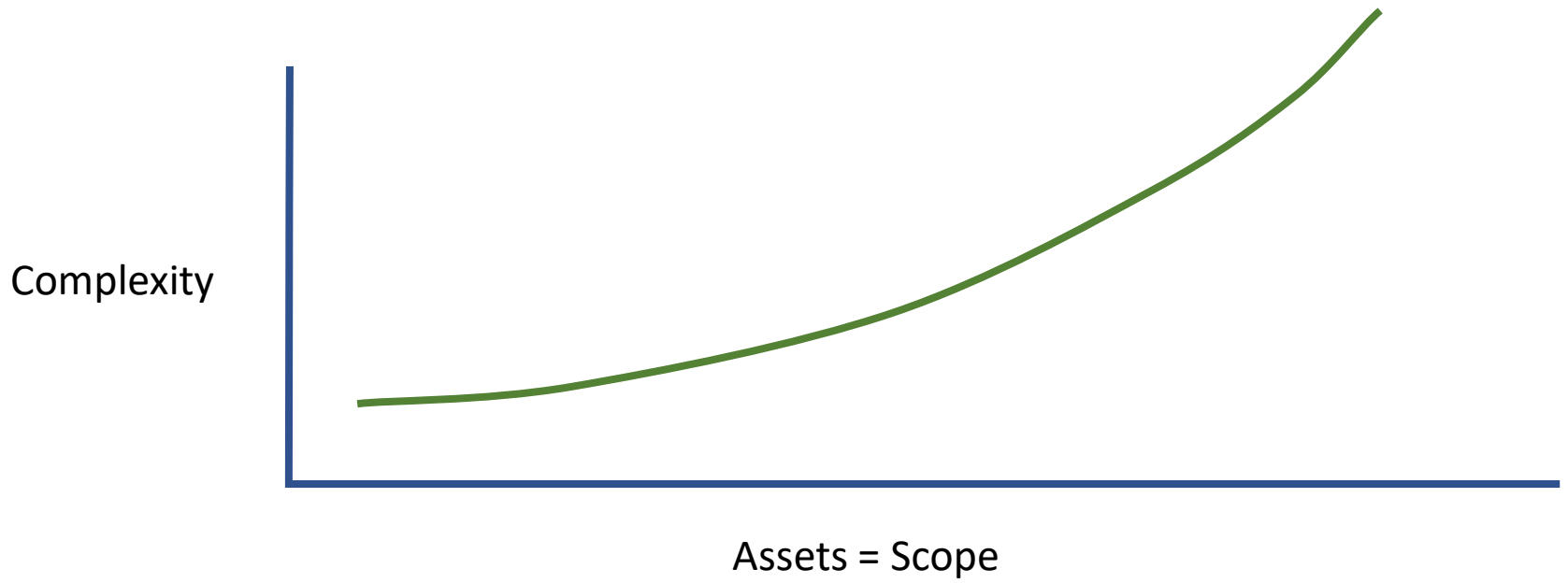
- document these assets in asset inventory;
- document these assets in the SSP to show they are managed using the contractor's risk-based security policies, procedures, and practices; and
- provide a network diagram of the assessment scope (to include these assets) to facilitate scoping discussions during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

Inventory | SSP | Network Diagram

CMMC Assessment Scope – Level 2 | Version 2.0; page 4

Information Protection Difficulty

Assets = Scope = CMMC Assessment Complexity



Operational Environment

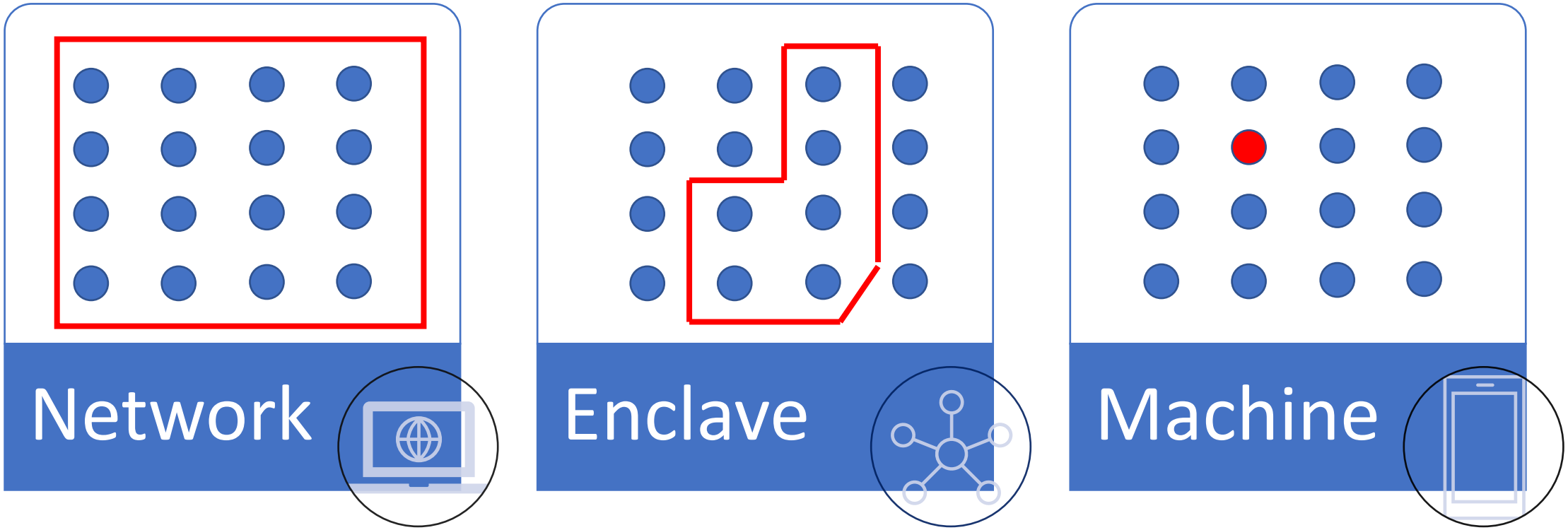
- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, 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**:

Guide for Developing Security Plans for Federal Information Systems, NIST 800-18 r1, pg 22

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.

44 U.S.C., Sec. 3542

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 *Determine if:*	
	3.1.1[a]	*authorized users are identified.*
	3.1.1[b]	*processes acting on behalf of authorized users are identified.*
	3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d]	*system access is limited to authorized users.*
	3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f]	*system access is limited to authorized devices (including other systems).*

NIST SP 800-171A ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION; page 9

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

NIST Special Publication 800-18 Revision 1; Guide for Developing Security Plans for Federal Information Systems

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 = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION; Appendix E

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)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	NFO
PL-4	Rules of Behavior	NFO
PL-4(1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*	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