Developing and Implementing Essential Security Policies, Practices, and Procedures

Marc N. Violante

Wisconsin Procurement Institute

November 4, 2022

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

Webinar Description

- Cybersecurity does not exist solely by virtue of regulations, contractual requirement, or because someone says that it is required. Cybersecurity requires a positive corporate environment, support, and effort to achieve the proper blend of knowledge, actions and both software and hardware. By themselves, these elements will provide a degree of cybersecurity. However, to achieve the level of cybersecurity required by DoD, companies must take time to develop and implement policies, practices, and procedures. This webinar will discuss the types of documentation that companies should develop during their planning, implementation, and operational phases of creating their cybersecurity programs.

Cybersecurity – current requirements

- 52.204-21 - Basic *Safeguarding* of Covered *Contractor Information* Systems (Nov 2021)*
- 252.204-7008[P] - COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)
- 252-204-7012 - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)*
  - SSP > POA > NIST 800-171 r2
  - cyber incident – “response activities”: investigate, collect, report
  - Malware
- 252.204-7019[P]/7020* – DoD Basic Assessment > SPRS

P – Provision applies to solicitations | * Flowdown requirements

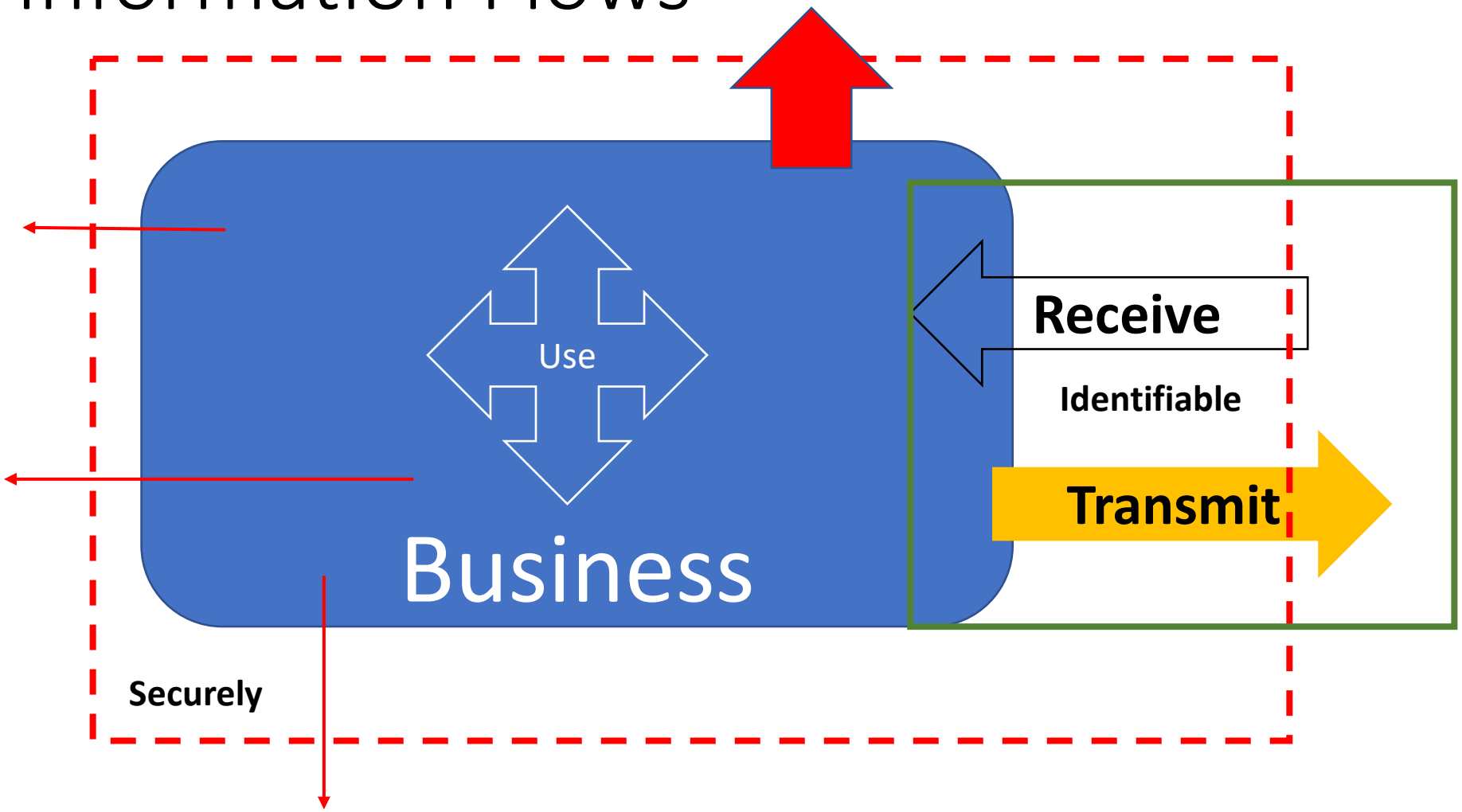
Securely

Focus of DFARS 252.204-7012/NIST 800-171 r2

- Confidentiality*
  - Information shared with designated and eligible recipients
- Integrity
  - Information remains in-tact
- Availability
  - Can access when needed

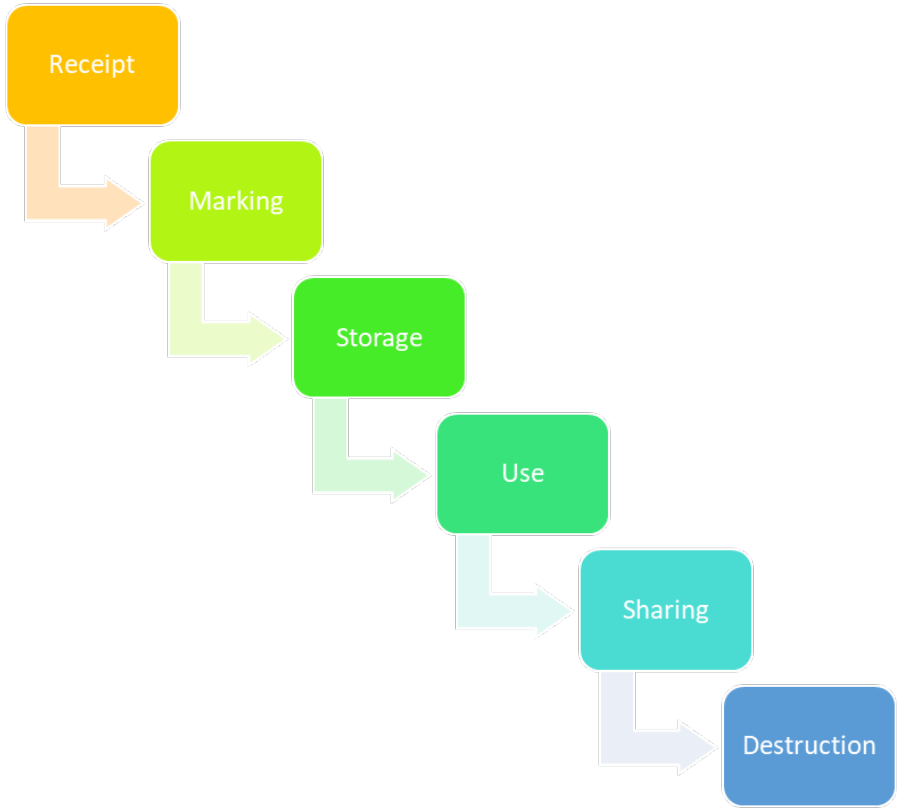
Start with the goal in mind.

Information Flows



Leakage/unauthorized transfer, sharing, and/or theft

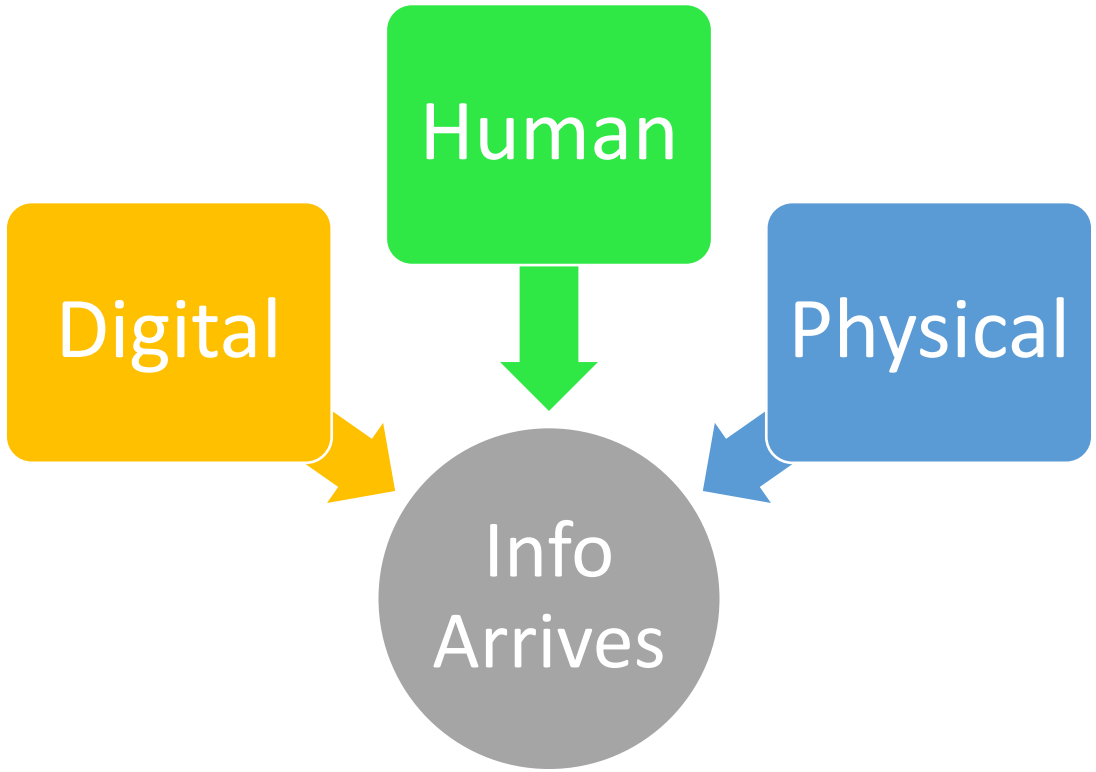
Information – life cycle, general elements



- Auditing
- Awareness
- Controls
- Deliverables
- Information – source(s)
- Monitor – test
- Questions to KO, other
- Training
- Transmittal registry
- Update procedures

M.N. Violante, WPI – Nov 2017

Information Flows - internal



- What pathways are used?
- Who uses?
- How is it protected?
- Where is it stored?
- How is it secured?
- How is it tracked?
- How is dissemination tracked?
- How is the process audited?
- How is information destroyed?
- Is there a Policy or Procedure?

System Specific Analysis

- System Characterization
- Threat Identification
- Vulnerability Identification
- Impact Analysis
- Likelihood Determination
- Control Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

Special Publication 800-30 Guide for Conducting Risk Assessments; Information Security Risk Assessment Toolkit, Mark Ryan, M. Talabis, Jason L Martin; Syngreess, pg 208

Notional Cybersecurity Risk Register

PRIORITIZING CYBERSECURITY RISK FOR ENTERPRISE RISK MANAGEMENT: NISTIR 8286B (DRAFT)

Notional Cybersecurity Risk Register											
ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											
Continually Communicate, Learn, and Update											

https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286B-draft.pdf, page 5 Comment Period: Sept 1 – Oct 15, 2021

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

Policies, Procedures and Practices

- Practice – statement of specific action/requirement
- Policy – "a set of guidelines, if you like –about how each type of data should be handled, validated and protected based on where it is traveling and who will be using it."[1]
- Procedures – detailed instructions which include what is to be done, when, how and by whom and if any special or require equipment is needed.

1. https://www.fcc.gov/sites/default/files/cyberplanner.pdf - How is that data handled and protected |

Best Practices - examples

- Verify links and files before clicking or downloading; both are common attack vectors for nation states, criminals, and insider threats.
- When clicking on hyperlinks in emails, hover over the link to verify authenticity. Also ensure that URLs begin with “https.” The “s” indicates encryption is enabled to protect users’ information.
- Always check the “To” and “Cc” line to ensure information is being sent to those with a need to know.
- Make passwords complex and change them frequently. Strong passwords include one uppercase letter, one lowercase letter, at least one number and 11 or more characters. Never write passwords down.
- Keep your computer healthy. This includes reading User Awareness Bulletins and acting as necessary to install software updates and apply security patches when prompted.
- Keep your Common Access Card (CAC) in your possession at all times. Your CAC serves as part one of two-factor authentication; it is something you have. Your pin, something only you know, serves as part two. A bad actor in possession of even one part of two-factor authentication increases the likelihood of access.
- Report phishing or suspicious activity. According to the National Cybersecurity Alliance, only 22 percent of email recipients report phishing. Utilize your Information Systems Security Manager and cybersecurity professionals for support.

https://www.navy.mil/Press-Office/News-Stories/Article/3183919/in-the-office-here-are-some-cybersecurity-est-practices-while-logged-on-to-a-n/

Policy v. Procedure

- Policies – “are guidelines that regulate organizations action. They control the conduct of people and the activities of systems.”
- Procedures – “are action oriented. They outline the steps you expect people to take and the sequence in which to perform those steps. They also frequently point out the consequences of failure to comply,…”
- “Never create a policy or procedure just to have one or because it seems like a good idea. Policies and procedures should *accomplish* something.”

Writing Effective Policies and Procedures – A Step-by-Step Resource for Clear Communication; Nancy J. Campbell, American Management Association 1998, pgs 1, 3, 5

Policies vs. Procedures

- A **policy describes** an organizational **goal and purpose**. Policies include guiding principles that inform and guide decision making. Policies include mission-oriented rules and requirements. Policies promote consistency and mitigate risk.
- **Procedures detail the process for accomplishing goals**, ensuring consistency. They include step-by-step descriptions of the tasks required to support and carry out organizational policies. **Procedures are subject to** change and **continuous improvement**.

https://armypubs.army.mil/Tools/PDF/Army_policy_writing_brief.pdf

Sample Policy Statements

Describes the goal ->

- Publications in any media will be authenticated by the appropriate official. Authentication constitutes clearance of the publication's content; verifies that appropriate coordination has been accomplished, including legal review; and clears the publication for issuance.
- Headquarters, Department of the Army principal officials will sign the DA Form 260 (Request for Publishing–DA Administrative Publications) for DA administrative publications publishing actions which hey are the proponent for before authentication by the SECARMY or designee.

Sample Procedural Statements

Describes actions ->

- When structuring departmental administrative publications—
  - Group the material by subject, identifying the individual topics to be covered.
  - Arrange the material logically. Material may appear in chronological order, by topic, in general-to-specific order, or in order of importance if the reader needs to know something about subject "A" in order to understand subject "B."
  - Divide large amounts of information into smaller pieces, such as chapters, sections, paragraphs, or subparagraphs. When subdividing an element, at least two of the same type must be used, as explained below.
- Before filing a record, examine it to ensure all actions are complete and essential information is attached. If essential information is missing and cannot be located, annotate the record indicating what measures are being taken to obtain the information. Envelopes, routing slips that bear no essential information and extra copies should be removed. Staple hardcopy documents when possible. Prior to stapling, documents should be assembled with the latest action on top. Other fasteners may be used when there are too many papers for stapling or physical characteristics prohibit stapling.

https://armypubs.army.mil/Tools/PDF/Army_policy_writing_brief.pdf

Example – Clean Desk Policy

Consensus Policy Resource Community

Clean Desk Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Last Update Status: *Updated June 2014*

1. Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt1e23a0c014d97cb9/5e9dda486a64bf2a22a10983/clean_desk_policy.pdf

Example – Clean Desk Policy elements

4. Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2 Computer workstations must be locked when workspace is unoccupied.

4.3 Computer workstations must be shut completely down at the end of the work day.

4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.7 Laptops must be either locked with a locking cable or locked away in a drawer.

4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt1e23a0c014d97cb9/5e9dda486a64bf2a22a10983/clean_desk_policy.pdf

Example – Clean Desk Policy -- Procedures

Clean Desk Procedures - MV

1. Remove all sensitive/confidential information in hardcopy or electronic form from the workplace and store in an authorized security container.
2. Verify the security container's status indicator to reflects – closed and locked prior to leaving and check to insure it is locked.
3. Lock your computer workstation when you will not be physically present.
4. Shut down completely your workstation at the end of the work day.
5. Empty or secure all waste/recycling receptacles prior to leaving.

From SANS Policy

4. Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2 Computer workstations must be locked when workspace is unoccupied.

4.3 Computer workstations must be shut completely down at the end of the work day.

4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.7 Laptops must be either locked with a locking cable or locked away in a drawer.

4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt1e23a0c014d97cb9/5e9dda486a64bf2a22a10983/clean_desk_policy.pdf

How to develop policy

Tenable security policy must be based on the results of a **risk assessment** as described in Chapter 2. Findings from a risk assessment provide policy-makers with an accurate picture of the security needs specific to their organization. This information is imperative because proper policy development requires decision-makers to:

- Identify sensitive information and critical systems
- Incorporate local, state, and federal laws, as well as relevant **ethical standards**
- Define institutional security goals and objectives
- Set a course for accomplishing those goals and objectives
- Ensure that necessary mechanisms for accomplishing the goals and objectives are in place

https://nces.ed.gov/pubs98/safetech/chapter3.asp

Policies – what to include

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws or regulations, if any, are the policy based on?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What information **assets** must be protected?
- What are users actually required to do?
- How should security breaches and violations be reported?
- ★ What is the effective date and expiration date of the policy?

List of effective Policies, revision number and effective dates

https://nces.ed.gov/pubs98/safetech/chapter3.asp

Example of a requirement

Access Control (AC)

Level 1 AC Practices

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

CMMC Assessment Guide – Level 2 | Version 2.0; page 12

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL - Procedures

- [SELECT FROM: Access control policy; procedures addressing
  - account management;
  - system security plan;
  - system design documentation;
  - system configuration settings and associated documentation;
  - list of active system accounts and the name of the individual associated with each account;
  - notifications or records of recently transferred, separated, or terminated employees;
  - list of conditions for group and role membership;
  - list of recently disabled system accounts along with the name of the individual associated with each account;
  - access authorization records;
  - account management compliance reviews;
  - system monitoring records;
  - system audit logs and records;
  - list of devices and systems authorized to connect to organizational systems;
  - other relevant documents or records].

CMMC Assessment Guide – Level 2 | Version 2.0; page 12

Documentation – general goals

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

- How do you prove _____?
- How do you show _____ ?
- How do you prove that access has been granted to authorized users?
- How do you show that access has been granted to authorized users?

General Framework - procedures

- What is required?
- Was it accomplished?
- By whom?
- How?
- When?
- Were the actions properly documented?

Periodicities

- Continuous
- As required
- Triggered by event
- Not applicable

Developing adequate evidence

- Data
- System record review
- System log review
- Externally created document
- Internally created document

Validation

- Review
- Hashed record
- System record
- Software record/report
- Internally generated with appropriate attestation
- Action documented by appropriate witness
- Action directly witnessed and documented

Identification/validation of Assets & Scope

- Listing
- Current
- Ownership
- Identified
- Referenced in applicable documents
- Record of changes
- Reference to applicable practices, procedures and policies

Reference material

- Current
- Available
- Specific to system elements
- Documentation
  - System created
  - Process created
  - Transaction created
  - Internally created
  - Verification procedures

Validation of Risk Assessment & Assignment

- Review of risk matrix
- Review of last risk assessment

Baseline Configuration

- Hardware
- Software
- Network access
- Training requirements
- Training completed & currency
- Determination of access required
- Access list appropriate entries

Sensitive Material Inventory

- Received
- Marked
- Transmitted
- Accessed - reviewed
- Accessed - In use
- Stored
- Destroyed
  - Record of destruction
  - Approved method/device

“Being a Word Miser”

- Use only the number of words necessary
- Think in Ones – one word is better than two.
- Two sentences are better than three.
- Some examples:
  - Use standard word order – subject-verb-object
  - Use parallelism
    - X Read the document, be sure to sign it, and then it must be returned to Personnel.
    - ✓ Read the document, sign it, and return it to Personnel
  - Be consistent
  - Use short words

Writing Effective Policies and Procedures – A Step-by-Step Resource for Clear Communication; Nancy J. Campbell, American Management Association 1998, pgs 84

Being a word Miser; continued

- Use common words
- Use short sentences (no more than 20 words) aim for 15.
- Use short paragraphs
- Use lots of lists
- Write as you speak
- Get rid of wordy phrases (In an effort to …, In the event that …)
- Get rid of pompous language
- Get rid of flabby language
- Watch adjectives
- Get specific
- Get rid of empty phrase (beginning of a sentence) There are … It is …

Writing Effective Policies and Procedures – A Step-by-Step Resource for Clear Communication; Nancy J. Campbell, American Management Association 1998, pgs 104-107

Plain Language Concepts

Be Clear	• Use plain language whenever possible; avoid jargon • Avoid overuse of acronyms (if used, make certain they are established upon first use) • Use the active voice • Organize and filter information with readers' needs in mind • Format the document so that it's easy to read and understand • Use tables or figures if that's the best way to show information
Be Concise	• Remove unnecessary words • Write sentences with 20 words or fewer and that contain a single thought, action, etc. • Use seven sentences or fewer per paragraph
Be Specific	• Include only information that the reader must know • Use words with precise meaning • Include details that are directly relevant to the main point

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/502513p.pdf?ver=2017-05-08-162106-670

Plain Language Objectives

Plain language is communication that your readers can understand the first time they read it.

In a plain language document, readers can achieve three objectives:

A. Find what they need;
B. Understand what they find; and
C. Use what they find to meet their needs.

https://www.esd.whs.mil/Portals/54/Documents/DD/plain_language/PlainLanguageCourse.pdf; Slide 5 of 44

Why Use Plain Language

A. Shows customer focus;

B. Communicates effectively;

C. Increases reader comprehension;

D. Reduces questions from readers;

E. Makes government services accessible; and

F. Increases readers' trust in government.

If F then ? ->CMMC – Increases assessor' trust in the cybersecurity capabilities of the business

https://www.esd.whs.mil/Portals/54/Documents/DD/plain_language/PlainLanguageCourse.pdf; Slide 8 of 44

Writing for your audience

1. Who is my audience?
2. What does my audience already know about the subject?
3. What does my audience need to know?
4. What questions will my audience have?

https://www.esd.whs.mil/Portals/54/Documents/DD/plain_language/PlainLanguageCourse.pdf; Slide 10 of 44

Organize the information

- Limit the document to five or six sections (about two per printed page).
- Add useful headings to help people skim and scan the page.
- Use lists to break up the text and outline steps in a process.
- Avoid having lists within lists or several levels of information.
- Use tables to make complex material easier to understand.
- Write short sentences and short sections to break up information into manageable chunks.

https://www.plainlanguage.gov/guidelines/design/

Use simple typography

- Use ragged right margins where possible, rather than centering or justifying your text.
- Set the leading (space between lines) to be 2 points larger than the type size. For example, 12 over 14.

Fonts

- Select a serif font for the body text (like Times Roman).
- Don't mix fonts within the body.
- Don't use more than two or three typefaces.
- Select a sans serif font for the headings (like Arial).

https://www.plainlanguage.gov/guidelines/design/

Headings and Bullets

Headings

- Use uppercase and lowercase (not all caps).
- Set headings in bold.
- Justify to the left margin.
- Triple-space before headings and double-space after (for example, 19.2 points before, 8.4 points after).

Bullets

- Use standard bullets (if you choose others, like diamonds or arrows, be consistent).
- Generally, don't use more than two types of bullets.
- Use numbers only if there is a sequence to identify.

https://www.plainlanguage.gov/guidelines/design/

Use tables to make complex material easier to understand – dense text

§ 163.25 Forest management deductions

1. Pursuant to the provisions of 25 U.S.C. 413 and 25 U.S.C. 3105, a forest management deduction shall be withheld from the gross proceeds of sales of Indian forest land as described in this section.

2. Gross proceeds shall mean the value in money or money's worth of consideration furnished by the purchaser of forest products purchased under a contract, permit, or other document for the sale of forest products.

3. Forest management deductions shall not be withheld where the total consideration furnished under a document for the sale of forest products is less than $5,001.

4. Except as provided in § 163.25(e) of this part, the amount of the forest deduction shall not exceed the lesser amount of ten percent (10%) of the gross proceeds or, the actual percentage in effect on November 28, 1990.

5. The Secretary may increase the forest management deduction percentage for Indian forest land upon receipt of a written request from a tribe supported by a written resolution executed by the authorized tribal representatives. At the request of the authorized tribal representatives and at the discretion of the Secretary the forest management deduction percentage may be decreased to not less than one percent (1%) or the requirement for collection may be waived.

https://www.plainlanguage.gov/guidelines/design/use-tables-to-make-complex-material-easier-to-understand/

Use tables to make complex material easier to understand – table version

§ 163.25 Will BIA withhold any forest management deductions?

We will withhold a forest management deduction if the contract for the sale of forest products has a value of over $5,000. The deduction will be a percentage of the price we get from the buyer. The following table shows how we determine the amount of the deduction.

If:	and:	then the percentage of the deduction is:
a tribe requests an increase in the deduction through a tribal resolution	they send us a written request	the percentage requested by the tribe
an authorized tribal representative requests a decrease in the deduction	we approve the decrease	the percentage requested, with a one percent minimum
an authorized tribal representative requests a waiver of the deduction	we approve the waiver	waived
none of the above conditions apply		the percentage in effect on November 28, 1990, or 10 percent, whichever is less.

https://www.plainlanguage.gov/guidelines/design/use-tables-to-make-complex-material-easier-to-understand/

Resources

- www.plainlanaguage.gov
- https://www.esd.whs.mil/Portals/54/Documents/DD/plain_language/PlainLanguageCourse.pdf
- http://www.sans.org/security-resources/policies/