CMMC – Are you ready?

Marc Violante

Wisconsin Procurement Institute

September 9, 2022

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

Registration Questions

- What is needed for compliance?
- Is a SPRS score of 110 (perfect) required for an SBIR?

- Any T&C's of an agreement/contract take precedence.

What is needed for compliance - today

- FAR 52.204-21 - ~ protecting Federal Contract Information (15)
- DFARS 252.204-7008 (P) – By submission of this offer …
- DFARS 252.204-7012 (C) – CDI (CUI) & Incident ID / Reporting
  - SSP | DoD Basic Assessment | POA
  - Paragraphs (c – g)
  - Paragraph (l) “does not abrogate” – JCP, ITAR, CUI, FCI, NOFORN, Other
  - Flowdown
- DFARS 252.204-7019 (P) – DoD Basic Assessment Assessments
- DFARS 252.204-7020 (C) – NIST Assessment Requirements / SPRS

Contractual Remedies to Ensure Compliance with DFARS Clause 252.204-7012

DFARS clause 252.204-7012 requires a contractor to implement, at minimum, the NIST SP 800-171 security requirements on covered contractor information systems. Contractors must implement all of the NIST SP 800-171 requirements and have a plan of action and milestones (per NIST SP 800-171 Section 3.12.2) for each requirement not yet implemented. Failure to have or to make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements. Remedies for such a breach may include: withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole. Contracting Officers should consult with legal counsel as well as the program office or requiring activity to discuss appropriate remedies for the specific circumstances surrounding individual contracts.

https://www.acq.osd.mil/dpap/policy/policyvault/USA000807-22-DPC.pdf, dated June 16, 2022

Be aware of subtle requirements

- Contracting Officers are also reminded, in accordance with DFARS 204.7303(b)(2), if a contractor is required by a contract containing DFARS clause 252.204-7012 to implement NIST SP 800-171 on a covered contractor information system relevant to a new contract, option exercise, contract extension or new procurement modification, task order, or delivery order; the Contracting Officer must verify, prior to award, the contractor has the summary level score of a current NIST SP 800-171 DoD Assessment for that system posted in SPRS. This requirement applies even if the new award does not include DFARS clause 252.204-7020.

https://www.acq.osd.mil/dpap/policy/policyvault/USA000807-22-DPC.pdf, dated June 16, 2022

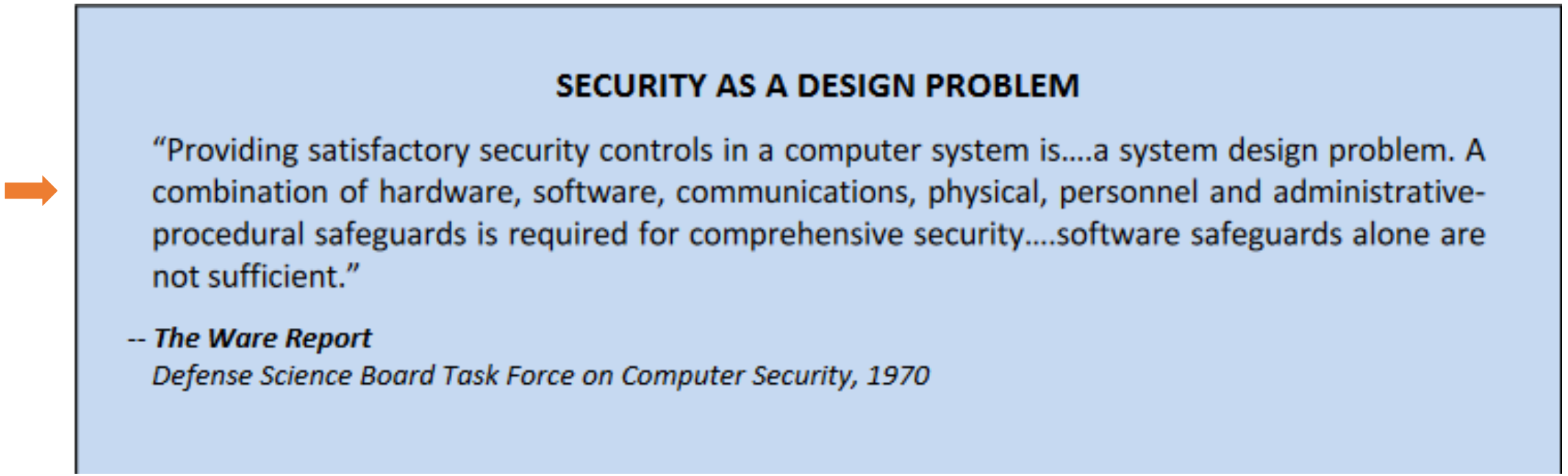
Webinar Description

September 9, 2022

- You have your System Security Plan, a Plan of Action, and have uploaded your DoD Basic Assessment score and associated information into SPRS. These are the core requirements which underpin both the current DoD Basic Assessment requirements and form the foundation for future CMCC requirements.
- The major differences between the Basic Self-assessment and CMMC are the level of formality applied to the management and administration of the program and the level of detail and discernment employed in conducting either an internal self-assessment for Level 1 and some Level 2 programs and for third-party assessments for all other Level 2 assessments. In all cases, DoD Suppliers should review their programs as an external reviewer would.
- The key questions that this webinar will address are:

1. What does that really mean?
2. How does a company successfully adopt the appropriate mindset?
3. What documentation is required and what is satisfactory level of detail?

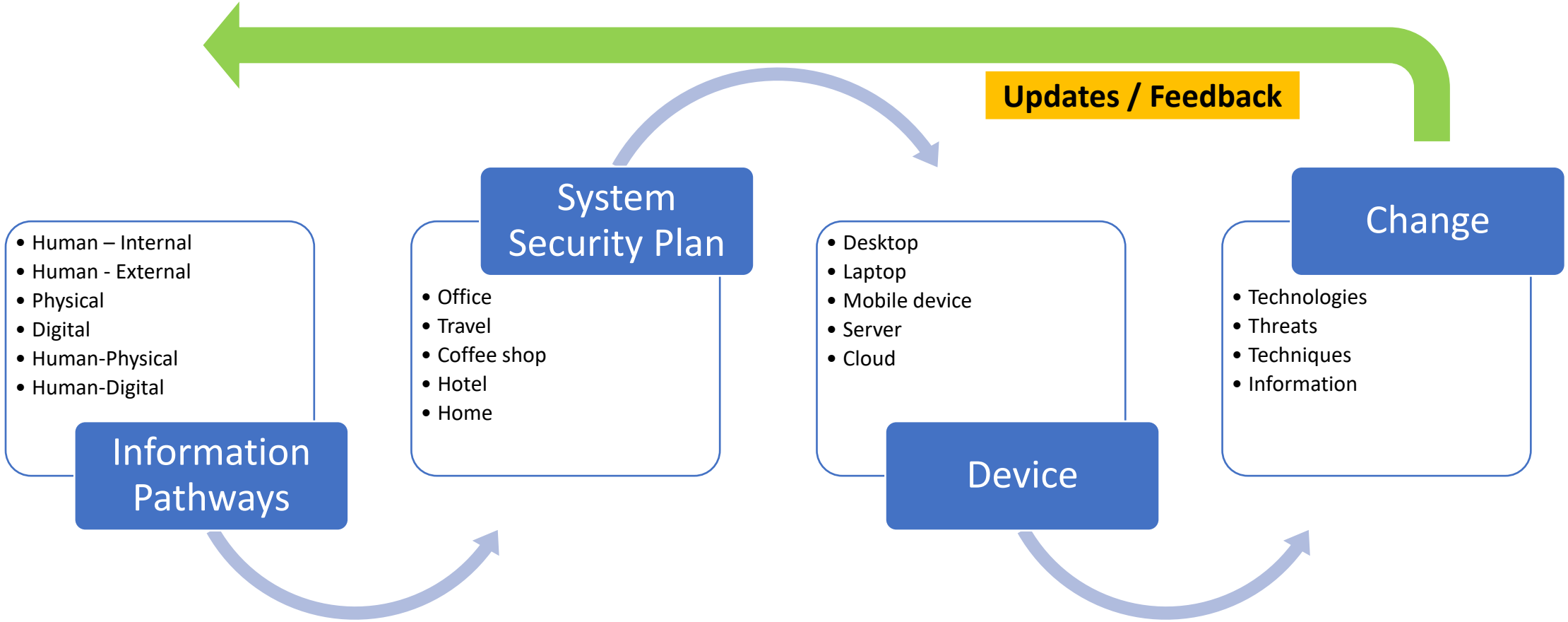
Solve the correct problem



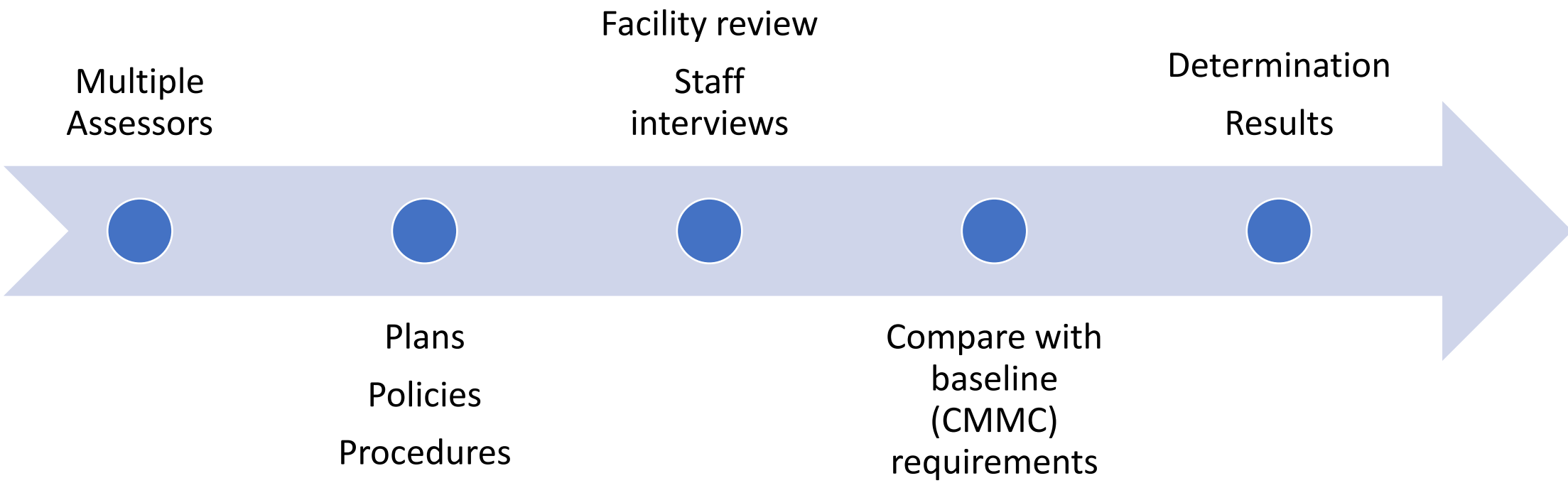
Security – a multidimensional problem

NIST 800-53, Chapter 2 – page 11

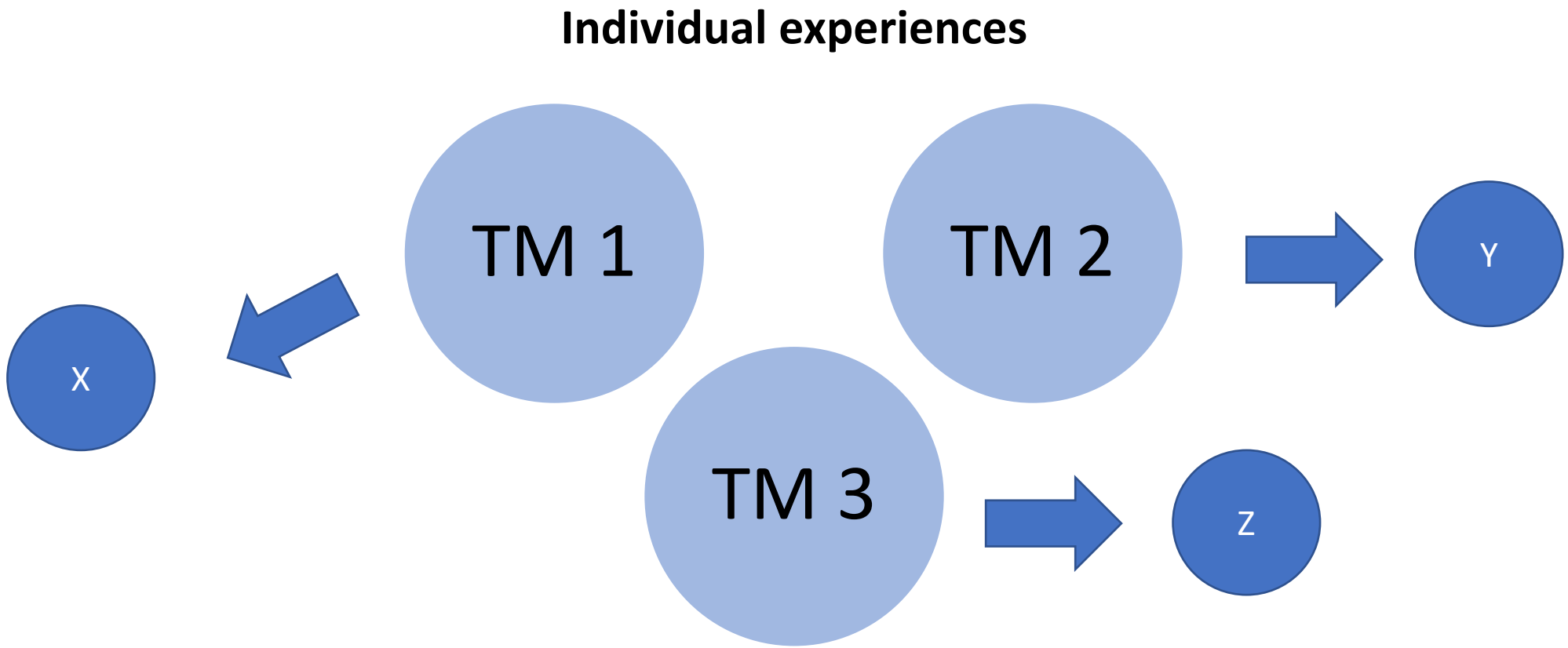
Dynamic/Evolving Environment



CMMC what has to happen?



Byproduct of the process



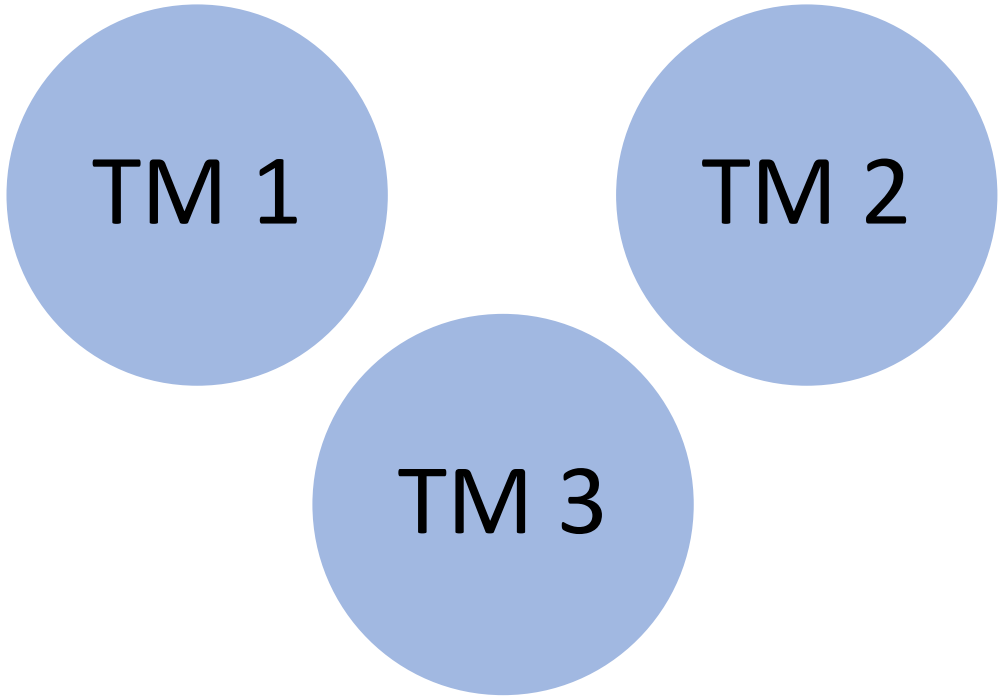
CUI Security Requirement Families

How will the assessment team manage the assessment?

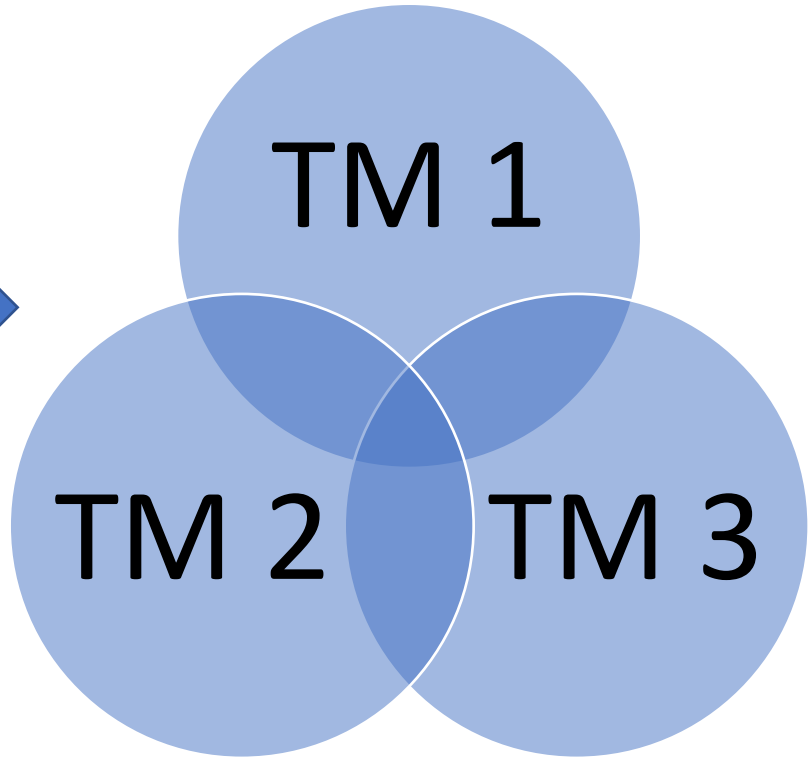
FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System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

The goal - Creating consensus

Individual experiences



Shared experiences

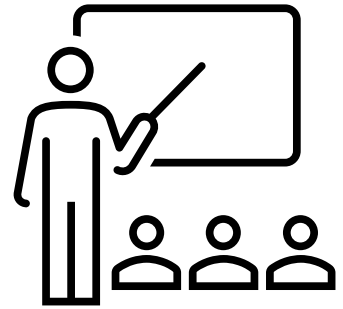


The Value of Standardization

- Helps to create a “value proposition”
- All elements communicate a central theme(s)
- The repetitive nature of the theme(s) is memorable
- More resilient to staff changes
- Allows for quicker response to internal & external changes
- Creates a cohesive structure for the program
  - All elements fit and integrate

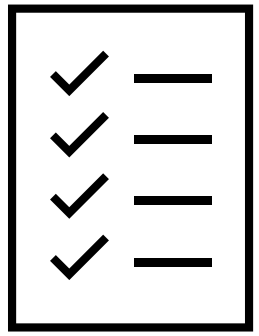
The Importance of Standardization

- Accelerate familiarity
- One learning curve
- Create sense of “comfort”
- Access appropriate information
- Extension of training
- Extension of institutionalization
- Reflect corporate support and vision
- Reflects that there are policies and procedures



Applicability of Checklists

- Consistency – removes personal element (knowledge, experience)
- Creates a reusable process
- Ensures all required elements are addressed
- Developed from corporate experience
- Does not rely upon memory
- Reproducible
- The Checklist Manifesto



Standardization – all aspects

Training

Document maintenance

Document creation

Document review

Adopt the mindset of the assessor

- Understand and/or attempt to understand their ---
  - Beliefs
  - Bias
  - Charter – DoD / The Cyber AB
  - Fact based
  - Interests
  - Goals
  - Outlook
  - Risk aversion
- They will need to collect/assemble evidence to support and to be able to defend their conclusion.

Thinking about CMMC

- What are you doing?
- Who is responsible?
- How are you doing it?
- Why are you doing it?
- Is evidence required?
- Is the required evidence being collected?
- Are the processes repeatable?
- Are the results verifiable?

A successful plan relies upon

- Being comprehensive
- Well resourced
- Periodic reviews and updates
- Adequately staffed
- Knowledgeable staff – trained & periodic retraining
- Validated
  - We want to know that it works, achieves the outcome – Adequate Security
  - To do that, we need to ID – gaps, holes, weaknesses

The W's of Information handling

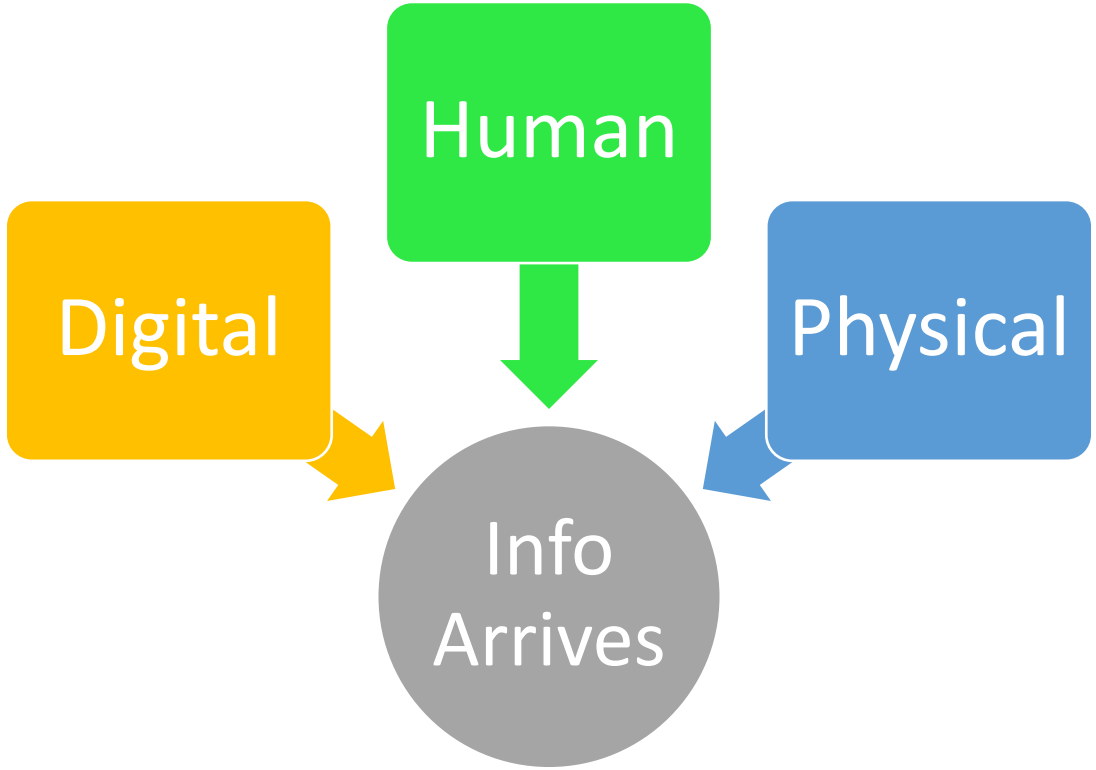
- What information do we have?
- What information do we use?
- With whom is information being shared?
- What information is being shared?
- What are the handling requirements?
- Where – how is the information being shared?
- When – normal hours / off hours
- Why is it being shared?
- Other questions ---

Dimensions to test

- Hardware
- Software
- Communications
- Physical
- Personal
- Administrative procedural safeguards

- “Software safeguards alone are not sufficient”

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?

SECURITY CONTROL ASSESSOR – for context

- The *security control assessor* is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). Security control assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, security control assessors prepare the final security assessment report containing the results and findings from the assessment. Prior to initiating the security control assessment, an assessor conducts an assessment of the security plan to help ensure that the plan provides a set of security controls for the information system that meet the stated security requirements.

Managing Information Security Risk Organization, Mission, and Information System View NIST 800-39, page D-7

Understand the assessment process

The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of the safeguards intended to meet the set of security requirements specified in NIST Special Publication 800-171. In this context, the information gathered and the evidence produced can be used by an organization to:

- Identify potential problems or shortfalls in the organization's security and risk management programs;
- Identify security weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- Prioritize risk mitigation decisions and activities;
- Confirm that identified security weaknesses and deficiencies in the system and in the environment of operation have been addressed; and
- Support continuous monitoring activities and provide information security situational awareness.

ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORM, NIST 800-171 A ; Chapter 1 page 1

Question everything

- It is said that there are two types of companies –
  1. Those that have been hacked.
  2. Those that have been hacked but don't know it.

- Some businesses claim that they have not been hacked –
  - OK – prove it.

Focus on the spirit & intent – not the words!

- It's not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage.

Hid for two years!

Internet Security Threat Report, Volume 21, April 2016, Symantec

When does the review begin?

- What is the first contact?
  - Email
  - Phone call
- What is discussed?
- What is the tone?
- Who takes the call?
  - Are notes taken?
  - Is the called identified?
    - How?
- Was anything documents requested?
- Was coordination information shared?
- Are the staff prepared?
- Is information readily available?
- How is it packaged?

First Impressions

- A review team arrives
  - What do they see?
  - What do they experience?
  - How are they received?
  - What questions may be asked?
  - Is the process used the norm or created just for them?
  - How are visitors greeted?
  - How will the team be greeting?
  - How will the team be identified? Badged? Escorts assigned?
  - Will there be a letter (email) sent with specific information?
    - These individuals will have access to company sensitive information – maybe the most sensitive

Plan, Policies, Procedures

- Is there a Master List?
- Is each document identified by revision number/date?
- Who signed the document?
  - If the signer is other than the CEO/President is there a Letter of Designation authorizing them to act on behalf of the company
- Have all applicable documents been reviewed/approved by the board or approval authority?
  - Formally approved
- Is the final document Hash'd?

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.

A CMMC imperative

Inventory | SSP | Network Diagram

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

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.

CMMC Self-Assessment Guide – Level 1 | Version 2.0; page 3

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

https://www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211202_508.pdf page 4

CUI Assets

CUI Assets process, store, or transmit CUI as follows:

- **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).

CUI Assets are part of the CMMC Assessment Scope and are assessed against applicable CMMC practices.

https://www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211202_508.pdf page 3

Understand the fine details

CUI SECURITY REQUIREMENTS

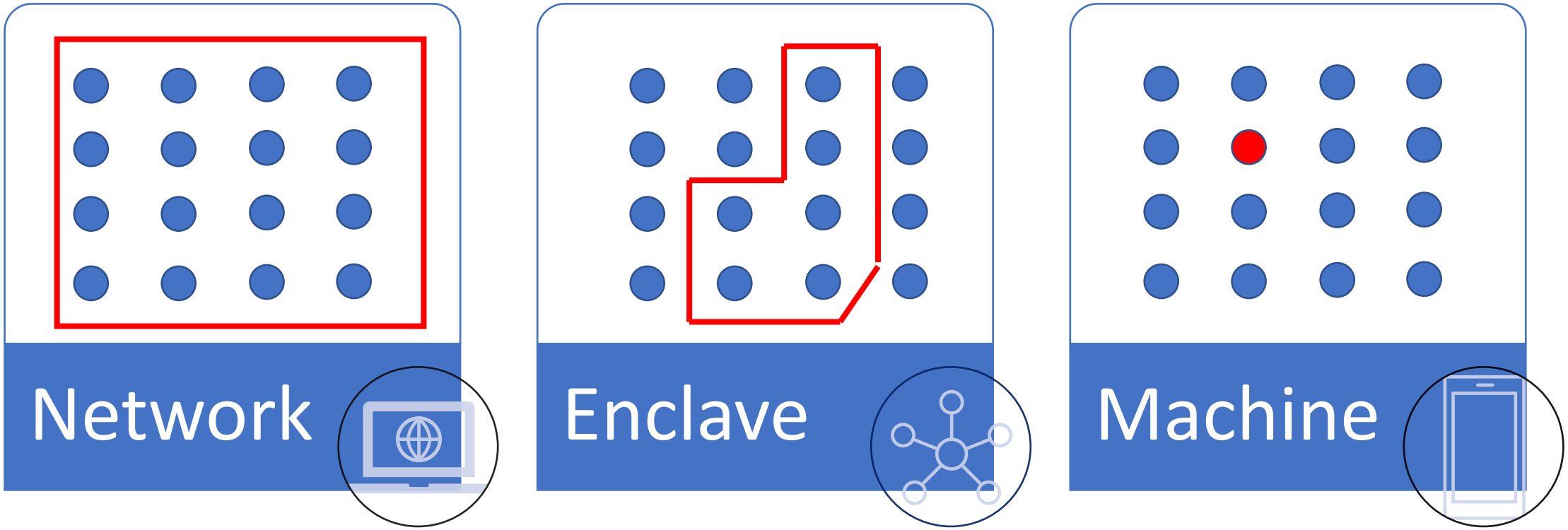
The recommended security requirements contained in this publication are only *applicable* to a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement. The security requirements apply to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION; NIST 800-171 r2 page: vii

Manage your scope

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.[9] If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

Determine needed participants



Risk Assessment

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

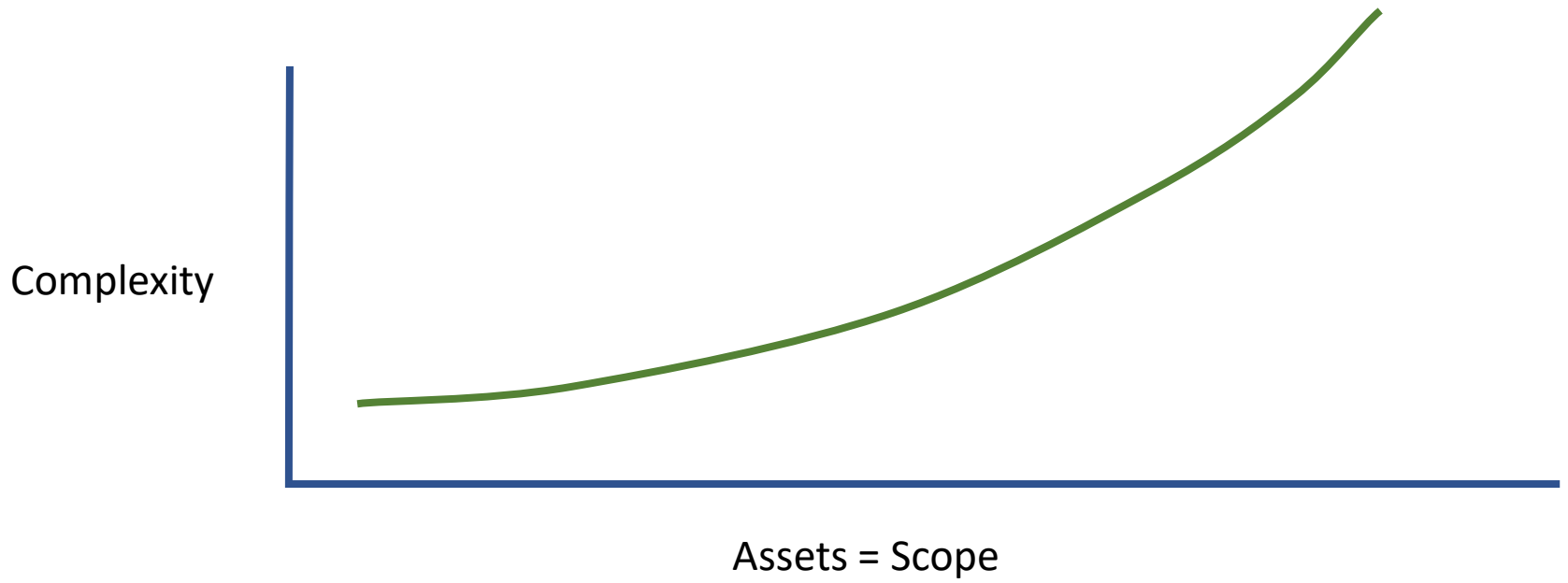
Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Month	New Entries	Modified Entries	New Vendors	New Products	Deprecated Entries
January	11,325	11,741	201	1,104	1,006
February	12,180	12,287	112	1,626	1,076
March	13,648	14,572	196	1,785	1,009
April	10,463	13,933	189	1,483	2,083
May	10,299	10,425	239	1,729	370
June	14,506	14,946	300	1,361	1,142
July	13,836	16,656	280	1,134	1,167
August	18,329	19,237	243	1,043	767
September	2,466	3,330	29	588	11

https://nvd.nist.gov/products/cpe/statistics

Information Protection Difficulty

Assets = Scope = CMMC Assessment Complexity



Manage your variables

- Staff
- Hardware
  - Computers – desktops, laptops, other – back-up drives
  - Network devices – routers, switches, servers, hubs
- Software
  - Administrative
  - Finance
  - Operations
  - Workflow

The Issue – an example

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).

Business Preparations

- Business Model
  - Aligns with “before, during and after” (Where do you fit? Who is your customer?)
  - Trust Model – Validated, Mediated, Mandated, Hybrid (NIST 800-39 app G)
- Data
- Delivery – knowledge of ability to perform
- Financial support -
- Program knowledge
- Registrations
- Resources – product, services, funding
- Risk management/responses – accept, avoid, mitigate, share, transfer (NIST 800-39, app H)
- Suppliers/subcontractors
- Transportation

Planning

- Should take an all-hazards approach
  - Physical
  - Staff
  - Equipment
  - Error
  - External threat
  - Malicious act, cyber
  - Other

"**Adequate security**" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. DFARS 252.204-7012

https://www.ready.gov/planning

Conduct rigorous regulatory analysis

- DFARS 252.204-7012
  - Adequate Security ~ at a minimum implement NIST 800-171 r2
  - Paragraphs c – g
  - Paragraph (l) – “does not abrogate”
    - FCI, CUI, JCP (Distribution Statements), ITAR, NOFORN, Other
  - DFARS 252.204-7000 Disclosure of Information
    - (a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

      (1) The Contracting Officer has given prior written approval;

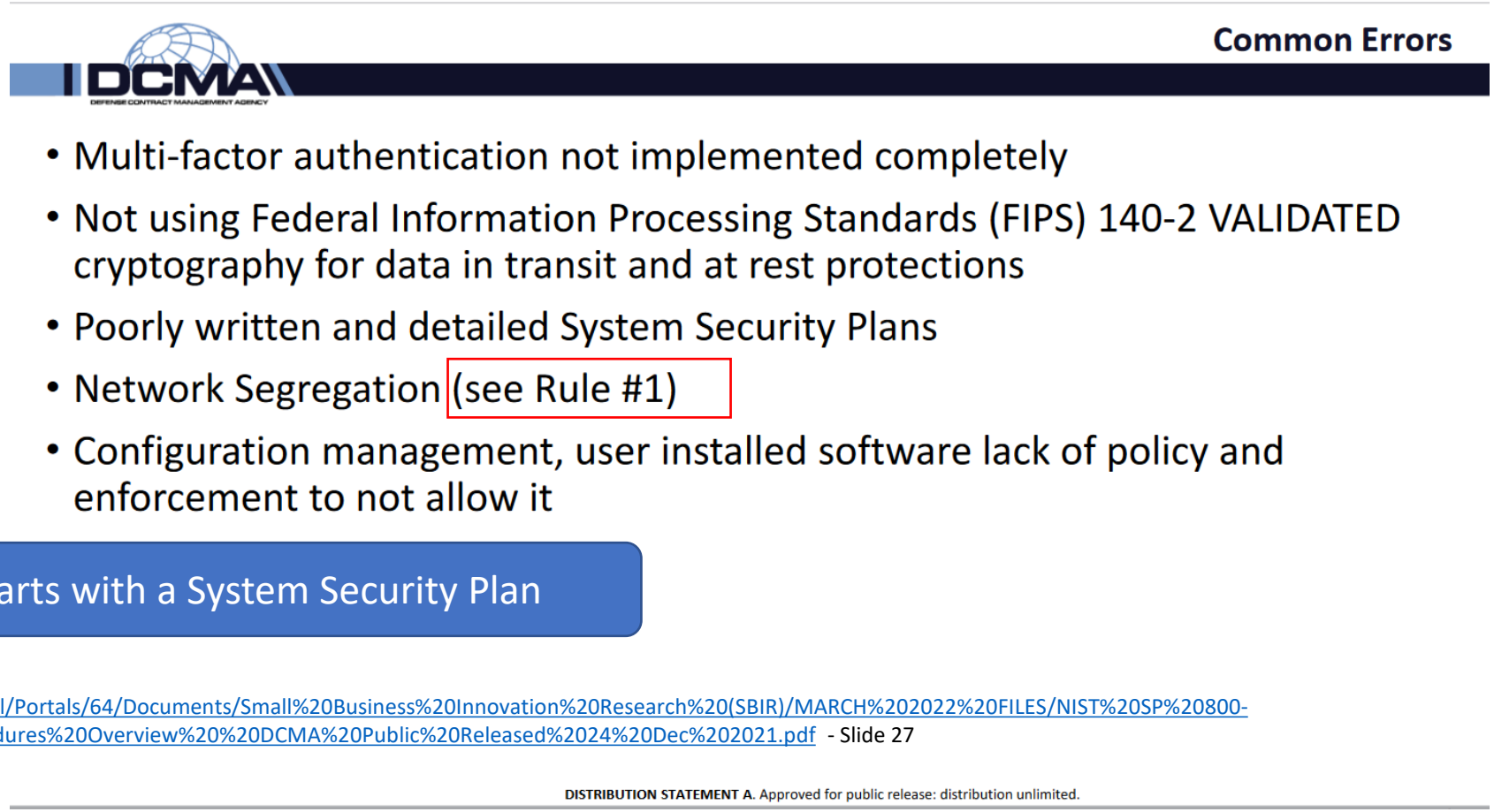
      (2) The information is otherwise in the public domain before the date of release; or
  - Flow-down requirements

Importance of the SSP & implementation

- (ii) Request a description of the contractor's implementation of the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident; and
- (iii) Provide a copy of the assessment of contractor compliance to the requiring activity, the DoD CIO at osd.dibcsia@mail.mil, and the other contracting officers listed in the cyber incident report.

https://www.acquisition.gov/dfarspgi/pgi-204.7303-3-cyber-incident-and-compromise-reporting.

DCMA identified Common Errors



Rule 1: It starts with a System Security Plan

https://www.safcn.af.mil/Portals/64/Documents/Small%20Business%20Innovation%20Research%20(SBIR)/MARCH%202022%20FILES/NIST%20SP%20800-171%20Policy%20Procedures%20Overview%20%20DCMA%20Public%20Released%2024%20Dec%202021.pdf - Slide 27

Change perspective

- From: We’re done; we have our SPRS score
- To:
  - How do we improve our plan?
  - How do we break our plan?
  - Are there holes in our plan?

Three Options

- Believe CMMC Ready and forget
- Question CMMC Readiness and conduct exercises
- Assume the role of the aggressor

Identify one flaw

- You don’t have to identify 1,000 cases
- 1 hole will sink a boat
- 1 security flaw will provide a potential adversary a pathway.

Change perspectives

- Conduct, threat analysis.
- Conduct, what could go wrong analysis?
- Develop risk-based approaches.
- Utilize cost impact analysis.
- Identify all assets and assign risk values

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Where to start

Utilize threat modeling

- Data-centric system threat modeling brings together the attack and defense side information for data of interest in a standardized model that facilitates
  - security analysis,
  - decision making, and
  - change planning.

Consider various threat types

- Adversarial – Individual, Group, Organization, Nation-state
- Accidental
- Structural
- Environmental
- *External reliance

Special Publication 800-30 Guide for Conducting Risk Assessments; Appendix D, D-2

Threat modeling

- Threat modeling is needed because of the dynamic nature of security. The attack and defense sides of 161 security are constantly changing. As part of handling this change, organizations should continually 162 reassess and evolve their defenses. This includes adopting continuous monitoring practices, security 163 automation technologies, and threat intelligence feeds to detect new vulnerabilities and attacks in near-164 real-time, allowing rapid risk mitigation. Another key component of handling the constant change in 165 security is having security metrics; these can be used for more informed decision making, again often 166 relating to risk management in general and risk mitigation in particular.
- Data-centric system threat modeling allows organizations to consider the security needs of each case of 474 interest, instead of relying solely on "best practice" generalized recommendations. Organizations are 475 already very familiar with applying best practices to operating systems and individual applications, such 476 as securing a web server (host) or web server software. What is considerably more challenging for 477 organizations to tackle is determining how to secure a particular chunk of data. It is not that securing a 478 piece of data is so difficult, but that traditionally security professionals, system administrators, and others 479 responsible for securing operational systems have focused on securing systems, not data. The rest of this 480 publication focuses on data security.

GUIDE TO DATA-CENTRIC SYSTEM THREAT MODELING (Draft) NIST 800-154, pg 9 & 10

Data-centric threat modeling

1. Identify and characterize the system and data of interest;
2. Identify and select the attack vectors to be included in the model;
3. Characterize the security controls for mitigating the attack vectors; and
4. Analyze the threat model.

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

Risk Assessment (three key aspects)

- Development of an information security architecture;
- Definition of interconnection requirements for information systems
- Design of security solutions for information systems and environments of operation including selection of security controls, information technology products, suppliers/supply chain, and contractors;

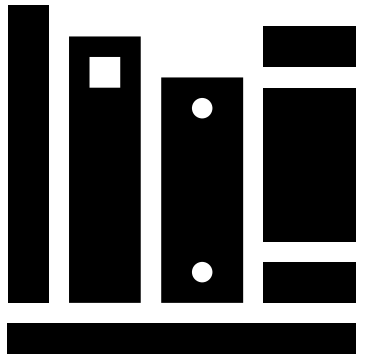
Special Publication 800-30 Guide for Conducting Risk Assessments; page 6

Develop Data Exchange Agreement

- Requirements – specifications
- Usage agreement
- Eligibility
- Protocols
- Software – encryption
- Identity – authorization
  - URL, Credentials, MAC

References

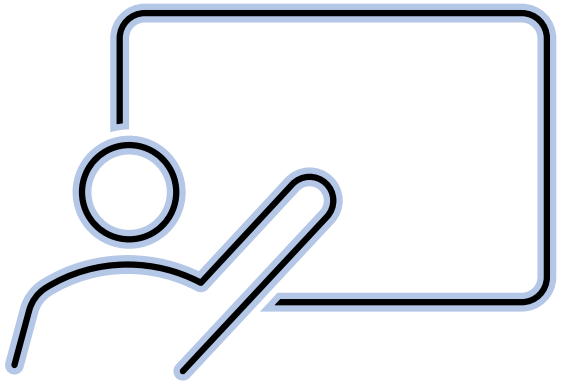
- Can there be a compliant program without the use of references?
- Are all references available?
- Is there a master list of references?
- Is each reference reviewed for being current?
- Is there evidence that they have been used?
- Are references cited in the materials?



Internal Audit

- List of items to review
- Periodicity
- Conducted by
- Training, experience, qualifications
- Findings/Status
- Schedule
  - Action items
  - Corrective actions
  - Tools for tracking?
- Final report
  - Designated official
  - Management review – comments, acceptance, signed out

Training records



- Are there training records?
- What documentation is included?
- Is there a master training schedule?
- Is training tailored based upon position?
- How are the training needs evaluated?
- How is the effectiveness of the training assessed?
- How are instructors/resources selected?
- Is there a company instruction – policy that addresses training?

Logs

- Visitor
- Training
- Internal Audits
- System activity – usage
- Maintenance
- Repair
- Upgrades
- Access
- Other

Review | Assessment Framework

- Is there a program assessment policy?
- Are responsibilities detailed?
- Are there required periodicities?
- Are formal reports submitted? To whom?
- Are deficiencies identified?
- Are action items identified?
  - Are they prioritized?
  - Are they tracked?
  - Are there repeat deficiencies?