CMMC: DFARS 252.204-7012; Information Security – Similarities and Differences

Marc Violante

Wisconsin Procurement Institute

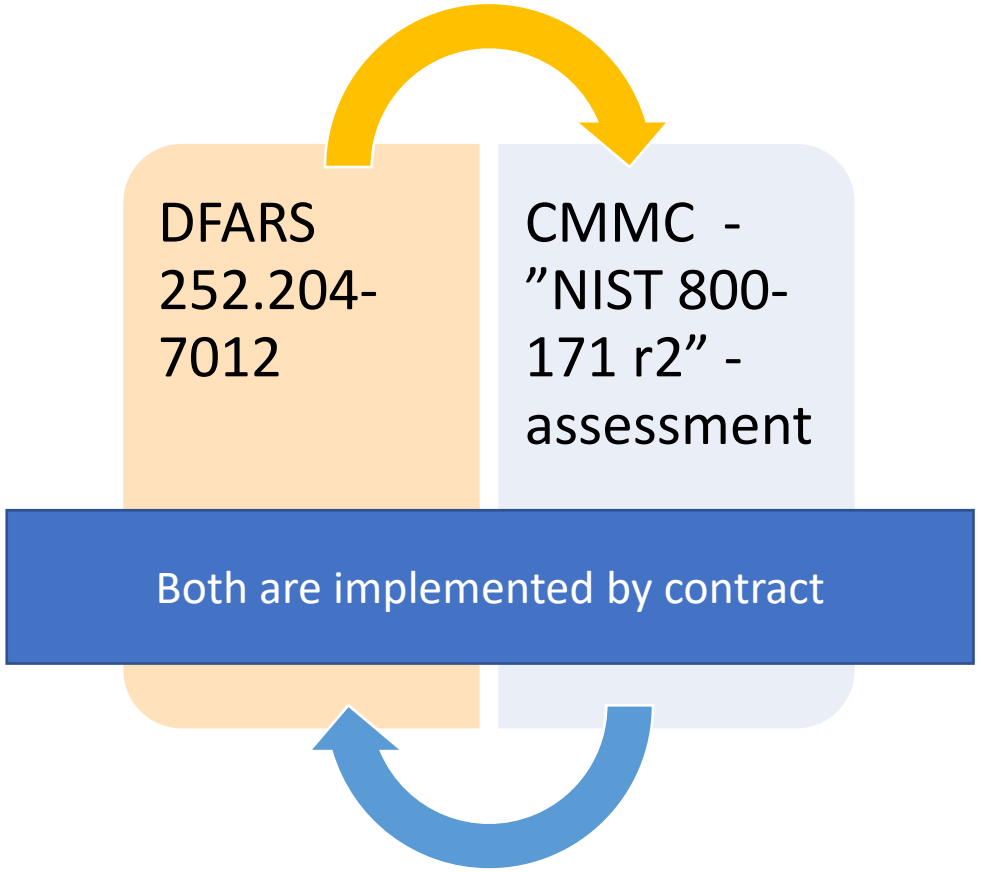
September 23, 2022

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

Webinar Description

A CMMC L1 or L2 certification does not guarantee compliance with all DFARS 252.204-7012 requirements and does not guarantee that a company will correctly handle other categories of information such as ITAR or JCP. The same is true about ITAR and CMMC. A fully functional ITAR compliance program will not begin to satisfy CMMC requirements. Ultimately, for each company to correctly handle different categories of information requires that they first know what information they are receiving and handling. Secondly, each company must have a detailed knowledge and understanding of each of the programs and program requirements.

Separate and Distinct but symbiotic



CMMC begins with a contract

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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION, pg vii

DFARS 252.204-7012 - 1

(c) *Cyber incident reporting requirement*.

(d) *Malicious software.*

(e) *Media preservation and protection*.

(f) *Access to additional information or equipment necessary for forensic analysis.*

(g) *Cyber incident damage assessment activities*.

(h) *DoD safeguarding and use of contractor attributional/proprietary information.*

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.*

DFARS 252.204-7012-2

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.*

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.*

In no way abrogates …

(m) *Subcontracts*.

DFARS - CMMC

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

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

Specialized Assets

- **Government Property** is all property owned or leased by the government. Government property includes both government-furnished and contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property or software [Reference: Federal Acquisition Regulation (FAR) 52.245-1].
- **IoT or Industrial Internet of Things (IIoT)** are interconnected devices having physical or virtual representation in the digital world, sensing/actuation capability, and programmability features. They are uniquely identifiable and may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors [Reference: iot.ieee.org/definition; National Institute of Standards and Technology (NIST) 800-183].
- **OT**[1] is used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems. OT may include programmable logic controllers (PLCs), computerized numerical control (CNC) devices, machine controllers, fabricators, assemblers, and machining.
- **Restricted Information Systems** can include systems [and associated Information Technology (IT) components comprising the system] that are configured based on government requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).
- **Test Equipment** can include hardware and/or associated IT components used in the testing of products, system components, and contract deliverables (e.g., oscilloscopes, spectrum analyzers, power meters, and special test equipment).

Identifying the CMMC Assessment Scope CMMC Assessment Scope – Level 2 | Version 2.0, page 5

CMMC Assessment Objectives

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;

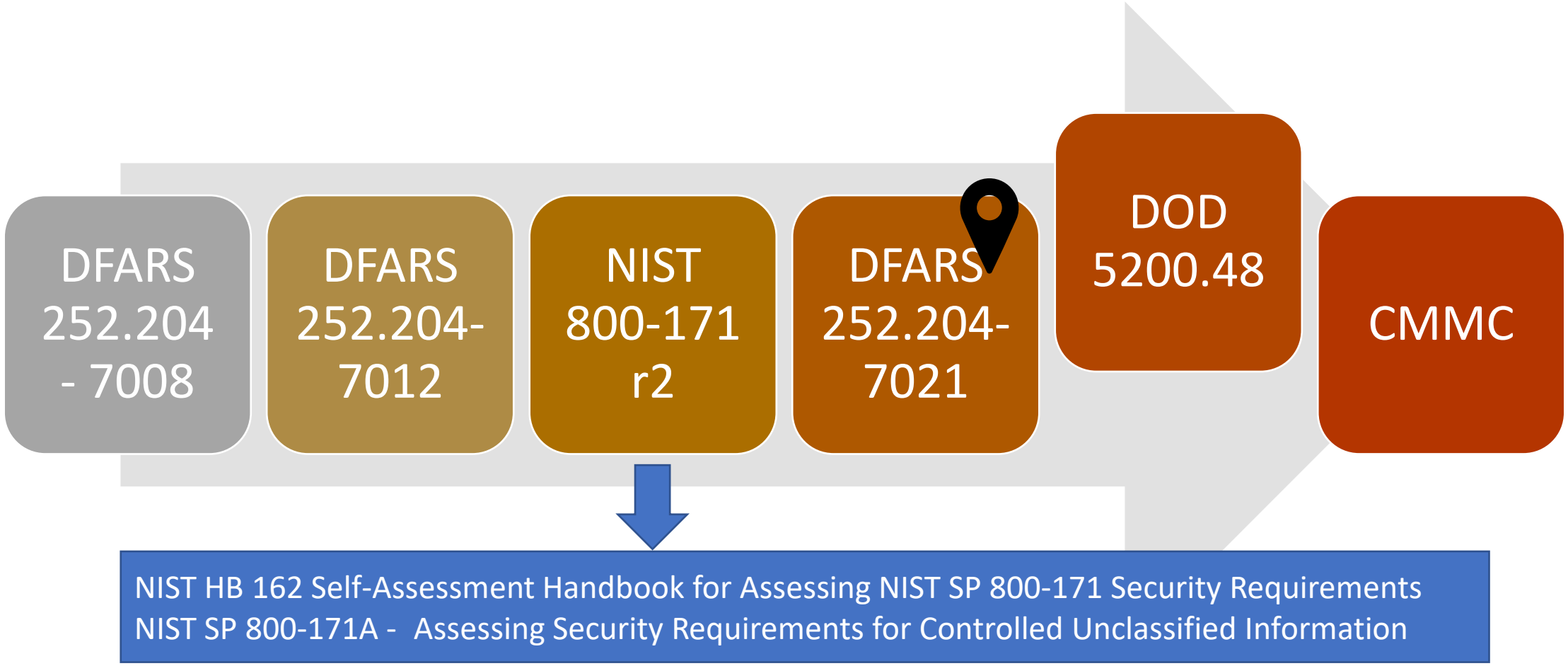
[d] system access is limited to authorized users;

[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).

CMMC Assessment Guide – Level 2 Version 2.0, pg 12

Getting to CMMC



Requirements

DFARS	NIST	CMMC	Other
• Protect CDI • Report • Other • Flow Down	• Scope • SSP • POA • Security Requirements	• Scope • Risk • Assets • Objectives	• Required training • Registration • Handling • Etc.

Requirements references (NIST 800-171 r2)

The requirements recommended for use in this publication are derived from [FIPS 200] and the moderate security control baseline in [SP 800-53] and are based on the CUI regulation [32 CFR 2002]. The requirements and controls have been determined over time to provide the necessary protection for federal information and systems that are covered under [FISMA]. The tailoring criteria applied to the [FIPS 200] requirements and [SP 800-53] controls are ***not*** an endorsement for the elimination of those requirements and controls; rather, the tailoring criteria focuses on the protection of CUI from unauthorized disclosure in nonfederal systems and organizations. Moreover, since the security requirements are derivative from the NIST publications listed above, organizations should ***not*** assume that satisfying those particular requirements will automatically satisfy the security requirements and controls in [FIPS 200] and [SP 800-53].

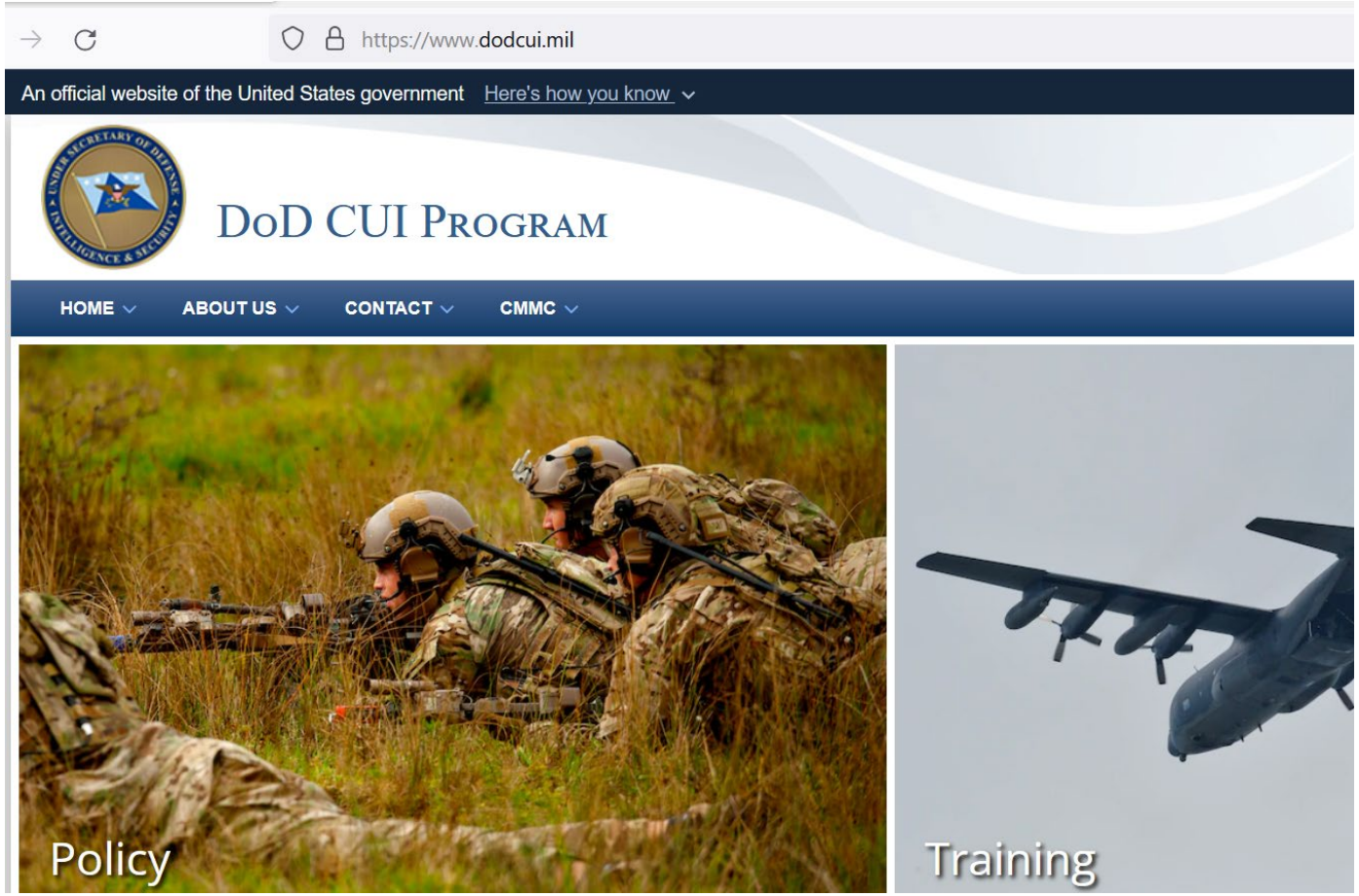
SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION, pg vi

SSP and POA

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. Nonfederal organizations develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and the plan of action as separate or combined documents and in any chosen format.[22]

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

DoD CUI Program



https://www.dodcui.mil/ - Home Page

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

DoD CUI Instruction 5200.48

DoD Instruction 5200.48

Controlled Unclassified Information (CUI)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	March 6, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Cancels:	DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security (USD(I&S))

Requirements for DoD Contractors

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf

Required CUI training

- In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training

DoDI 5200.48, March 6, 2020 SECTION 3: P ROGRAMMATICS pg: 17-18

DOD 5200.48 Requirement

https://www.dodcui.mil/Home/Policy/

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

DFARS 252.204-7012 general elements

DFARS 252.204-7012 v. CMMC

DFARS 252.204 - 7012

- Adequate Security
  - At a minimum NIST SP 800-171 r2
- Cyber Investigatons, data capture
- Cyber Incident Reporting
- Flow Down requirement

CMMC

- Implementation of NIST SP 800-171 r2
- CMMC L1/L2a – attestation
- CMMC L2b – third party assessment
- CMMC L3 – third party assessment + DIBCAC

The effect of CMMC

- CMMC Evaluates the implementation of NIST 800-171 r2
- CMMC does not formally or directly evaluate all elements of DFARS 252.204-7012
- There is some cross-over between DFARS 252.204-7012 & NIST 800-171 r2
- DFARS 252.204-7012 requires "the contractor to provide adequate security" – this includes "at a minimum" NIST 800-171 r2
- "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

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

DFARS 252.204-7012 (Adequate Security)

- (b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

  (1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

  (i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010 , Cloud Computing Services, of this contract.

  (ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

  (2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

  (i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

  (ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

Notice of broad information safeguarding requirements

- DFARS (l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.
- NIST 800-171 r2 – "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. " page iii

Information Handling Considerations

- 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 ---

Information types v. handling requirements

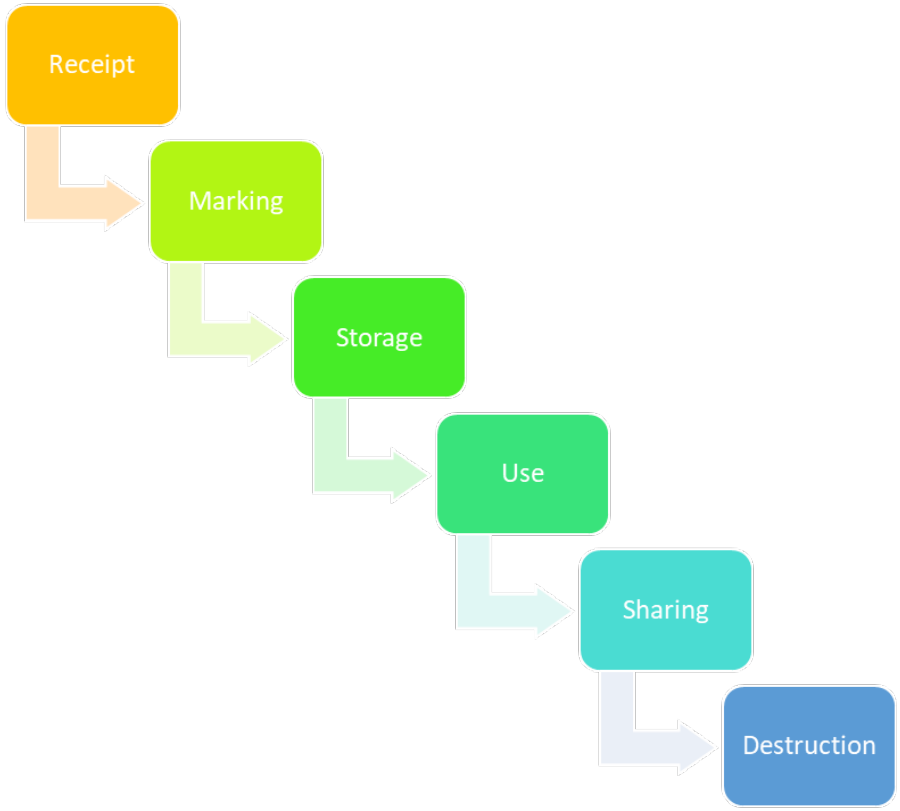
CUI	ITAR	JCP	Customer (x) – IP	Corporate – IP
• Lawful Governmental Purpose • DOD Required Training • DFARS 252.204 – 7012 / Basic Assessment, SPRS	• US Person – US Person • Registration • ITAR Compliance Program	• Data Custodian – Data Custodian • SAM, PIEE, DOD Basic Assessment, SPRS, DFARS 252.204-7012		

Importance of marking non-government information

(h) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

DFARS 252.204-7012

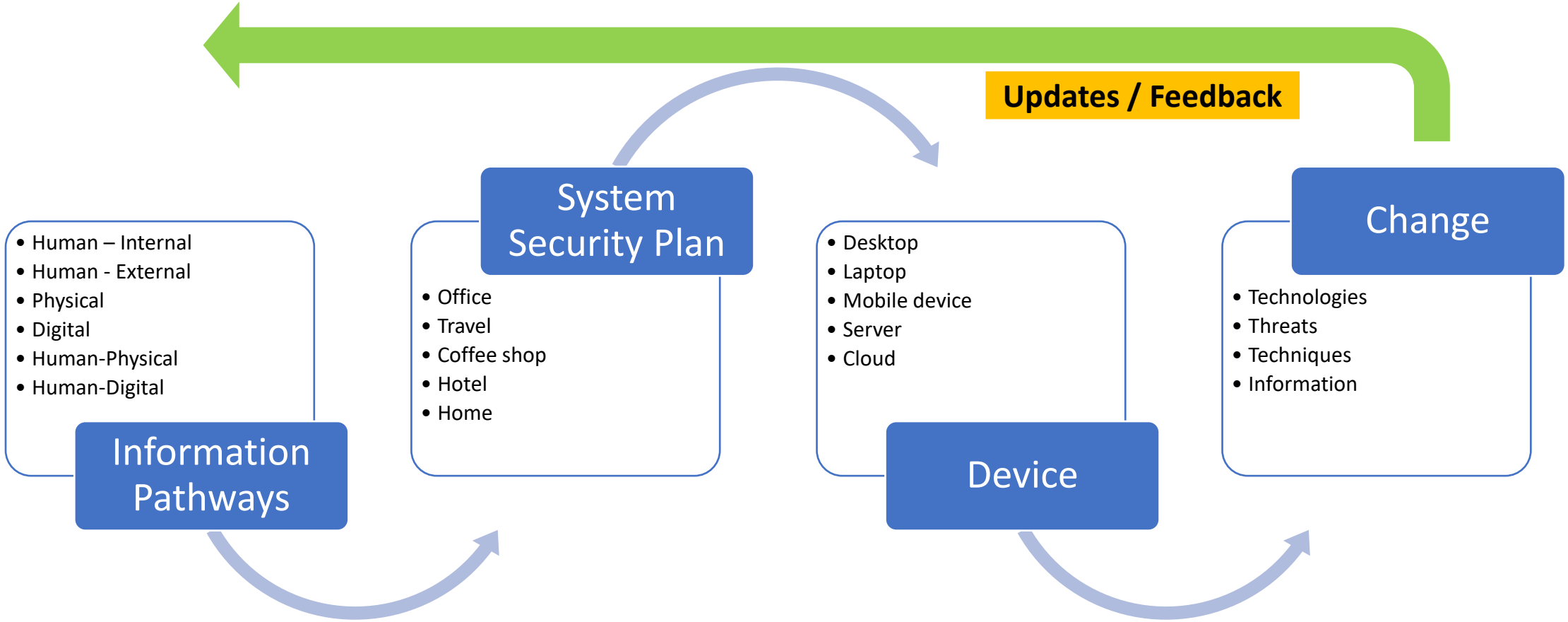
Information – life cycle, general elements



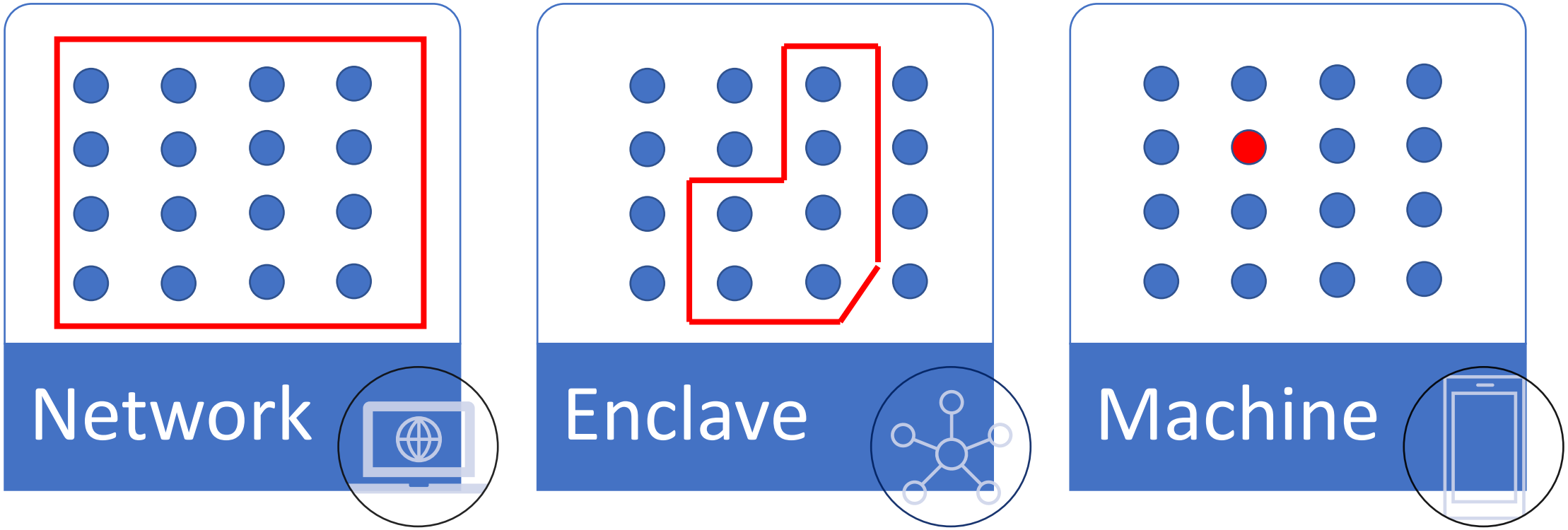
- Auditing
- Awareness
- Controls
- Deliverables
- Information – source(s)
- Monitor – test
- Questions to KO, other
- Training
- Transmittal registry
- Update procedures

M.N. Violante, WPI – Nov 2017

Dynamic/Evolving Environment

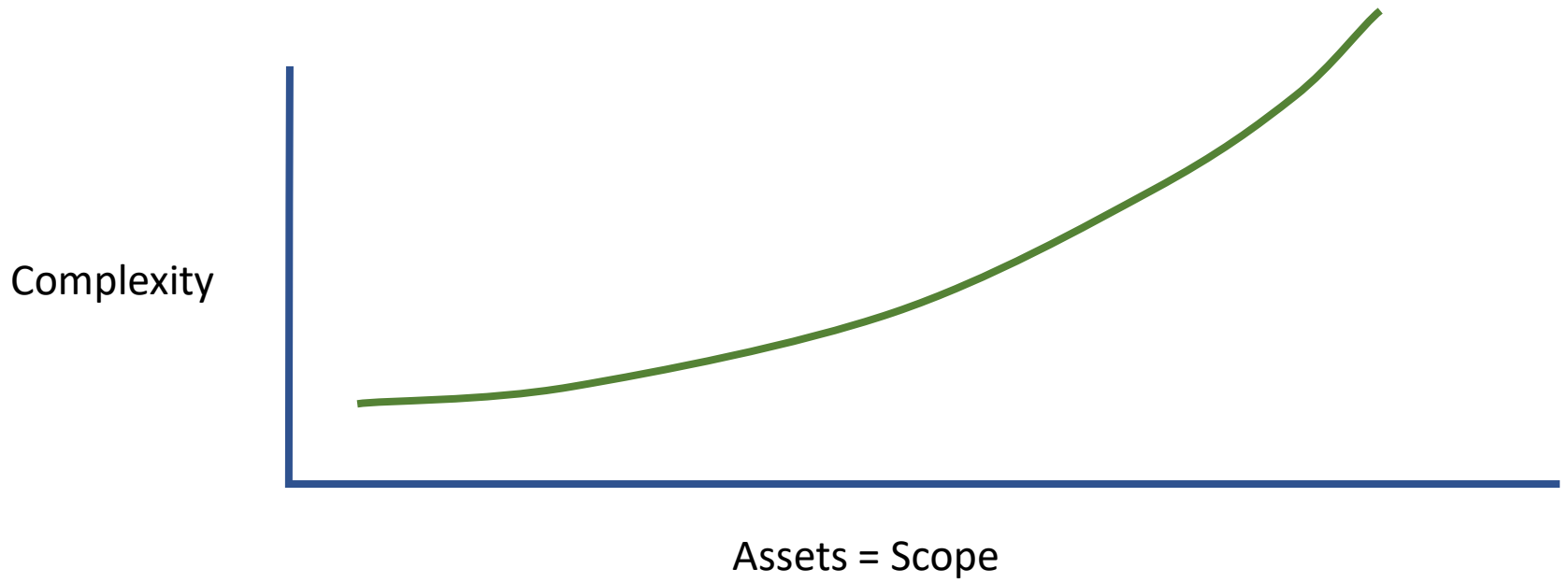


Determine needed participants



Information Protection Difficulty

Assets = Scope = CMMC Assessment Complexity



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

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

Determine 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.

SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION, Chapter 1, page 2

Defining Assessment Scope

The following asset categories are part of the CMMC Assessment Scope:

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

Identifying the CMMC Assessment Scope CMMC Assessment Scope – Level 2 | Version 2.0, page 6

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

CMMC Assessment Objectives

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).

CMMC Assessment Guide – Level 2 Version 2.0, pg 12

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

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

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

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

NIST/CMMC v. DFARS - evidence

3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

(e) ***Media preservation and protection***. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
(f) ***Access to additional information or equipment necessary for forensic analysis***.Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.
(g) ***Cyber incident damage assessment activities***. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

Cyber Incident Reporting

CMMC - 3.6.2 - Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. NIST SP 800-171 r2

DFARS –

- When the Contractor discovers a cyber incident that …
- Conduct a review for evidence of compromise of covered defense information
- Rapidly report (with in 72 hrs) cyber incidents to DoD at https://dibnet.dod.mil.
- Use the specified format
- Requires a Medium Assurance Certificate

Cyber incident report - 1

1. Company name
2. Data Universal Numbering System (DUNS) Number
3. Facility CAGE code
4. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)
5. Company point of contact information (name, position, telephone, email)
6. U.S. Government Program Manager point of contact (name, position, telephone, email)
7. Contract number(s) or other type of agreement affected or potentially affected
8. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
9. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support

Cyber incident report -2

12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative (Ex: Chronological explanation of event/incident, threat actor TTPs, indicators of compromise, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred)
20. Any additional information