PUBLIC CONTRACTING INSTITUTE

Protecting Sensitive Information and Proving it Through CMMC

Jim Goepel
General Counsel
Continuous Compliance LLC
JGoepel@FutureFeed.co

FutureFeed

About Jim Goepel

- General Counsel and Director of Education at FutureFeed
- Author of 2 books on Controlled Unclassified Information (https://CUIInformed.com)
- Founding Director of the CMMC Accreditation Body (Cyber AB)
  - Created and taught the RP program
  - Board Treasurer
- Co-author of Certified CMMC Professional (CCP) curriculum
- Co-Founder of the CMMC Information Institute
- Adjunct Professor at RIT; former Adjunct at Drexel University
- Expert Witness in Government Contracts Cases
- BSECE – Drexel University
  - Designed satellite test equipment and processes
  - Systems Administrator and Developer for the US Congress (House of Representatives)
- JD and LLM – George Mason University
  - Advisor to many government contractors including Unisys and JHU/APL
- Certifications:
  - Certified CMMC Assessor (CCA), CMMC Provisional Instructor, Certified CMMC Professional

Bottom Line Up Front:

- All organizations have sensitive information.
- Sensitive information needs to be properly safeguarded.
- Frameworks establish minimum safeguards for sensitive information.
- Responding to and, reviewing, cybersecurity questionnaires is economically inefficient.
- Third-party validation (i.e., assessments and certifications) allows for cost-effective, consistent validation of your supply chain.
- CMMC certifications are third-party validations trusted by the United States Department of Defense for those handling DoD sensitive information.
- CMMC certifications represent an economically efficient way of ensuring your organization will properly safeguard sensitive information.

Protecting Sensitive Information

What Makes this Information Sensitive?

There is a:

- legal
- regulatory
- contractual,
- ethical/moral, or
- business-based

obligation to safeguard it.

What are examples of "Sensitive Information"?

- Personally Identifiable Information ("PII")
- Personal Healthcare Information ("PHI")
- Employee bank account information
- Employee social security numbers
- Personnel records
- Intellectual property
- Business plans/roadmaps
- Vendor/partner information
- Customer information

Most Commercial Contracts

Require you to safeguard the other party’s sensitive information with:

- The same safeguards used to protect your own information; and
- Not less than reasonable care.

What is “Reasonable Care”?

Reasonableness

What would a reasonably prudent person do in a similar situation?

PUBLIC CONTRACTING INSTITUTE

Proving Reasonableness

Battle of the experts

- expensive
- lengthy
- prone to issues

Avoiding the Battle:

Use an established industry best practice, standard, or framework.

They bring with them increasingly stronger “reasonableness” due to the level of industry consensus/adoption.

Best Practices, Standards, and Frameworks

Best Practices vs Standards vs Frameworks

Serve similar purposes, but there are critical differences:

- Best Practice – industry consensus, but not typically formalized
- Standard – Contain implementation-specific details, but therefore can be unnecessarily restrictive or have unintended consequences for your organization
- Framework – high-level architecture designed to allow more flexible implementation than standards, but their lack of specificity can make implementation challenging

Choosing a Framework

Ideally, choose one that:

1. is used for similar purposes;
2. has seen/will see broad adoption;
3. has a well-established assessment processes; and,
4. has independent, third-party assessors/auditors.

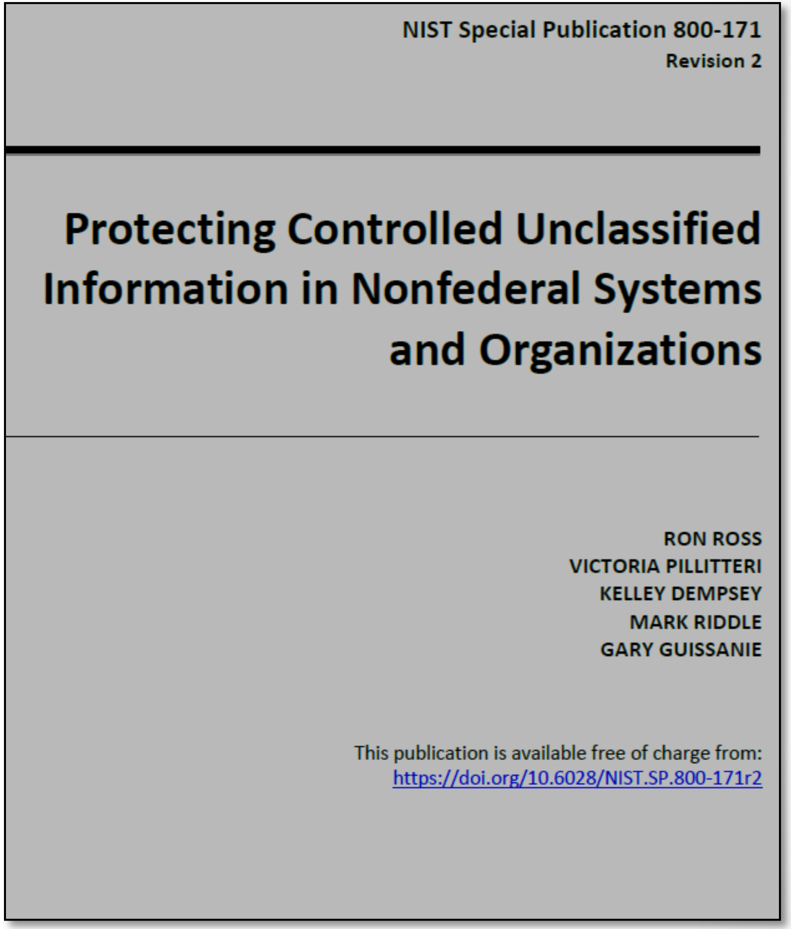
Public Contracting Institute

Cybersecurity Frameworks to Consider

Framework	Target Audience	Advantages	Disadvantages
System and Organization Controls ("SOC") 2	Commercial entities	• Based on a comprehensive set of "trust principles" • Flexible design • Well-recognized in the industry	• No clear set of requirements • Each organization designs its own controls, and compliance is measured against those controls • SOC reports are not certifications and can be difficult to analyze
Center for Internet Security ("CIS") Controls	Small and Medium Businesses	• Limited number of requirements • Helpful implementation guidance available	• Not robust • Less likely to properly protect sensitive information • Limited adoption
National Institute of Standards and Technology ("NIST") Cybersecurity Framework	Critical Infrastructure Organizations [includes defense contractors]	• Provides an excellent framework for defining corporate cyber risk and designing a comprehensive cyber program	• Requires a LOT of thoughtful consideration before implementation begins • Can be difficult for SMBs to implement • Limited adoption
NIST Special Publication ("SP") 800-53	U.S. Government Agencies	• Provides a comprehensive approach for implementing a cyber program based on organizational risk	• Requires extensive knowledge and expertise to properly implement • Significant (multi-year) implementation timelines • Expensive to implement • Limited adoption
NIST SP 800-171	U.S. Government Contractors handling Controlled Unclassified Information ("CUI")	• Specifically designed for the safeguarding of sensitive information • Will soon be adopted by 80,000+ organizations worldwide	• Requires allocation of significant resources (people, money, time) to properly implement • Likely to have a short-term, negative impact on operations • Focuses on confidentiality

NIST SP 800-171

- Establishes the minimum required protections that must be in place to safeguard Controlled Unclassified Information.
- 110 requirements designed to give contractors flexibility during implementation while still safeguarding sensitive information.
- All federal agencies are supposed to require their contractors who handle Controlled Unclassified Information (“CUI”) to implement NIST SP 800-171.



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

What Makes Information CUI?

- Information
  - the Government creates or possesses,
  - or that an entity creates or possesses for or on behalf of the government,
  - that a law, regulation, or government-wide policy [“LRGWP”] requires or permits an agency to handle using safeguarding or dissemination controls.

[LRGWP definition added]

NIST SP 800-171 is Designed to Protect CUI

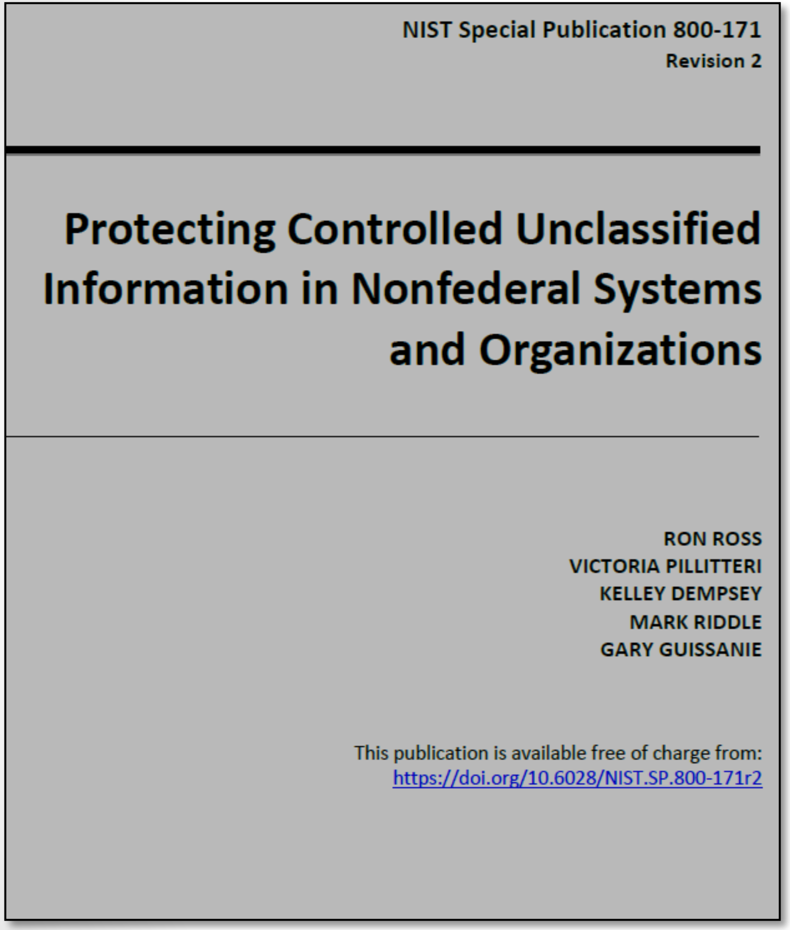
Sensitive Information

- Personally Identifiable Information ("PII")
- Personal Healthcare Information ("PHI")
- Employee bank account information
- Employee social security numbers
- Personnel Records
- Intellectual property
- Business plans/roadmaps
- Vendor/partner information
- Customer information

Controlled Unclassified Information ("CUI")

CONTROLLED UNCLASSIFIED INFORMATION

- Personally Identifiable Information ("PII")
- Personal Healthcare Information ("PHI")
- Bank records
- Social security numbers
- Personnel Records
- Intellectual property
- Budget
- Proprietary Information
- Citizens' Information
  - Net worth
  - Retirement
  - Student records



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST SP 800-171

- Designed to protect sensitive information that is similar to the information most organizations handle.
- Due to DoD’s CMMC program, will soon be adopted by at least 80,000+ contractors worldwide, including SMBs.
- This makes it hard to beat as a framework for establishing “reasonableness.”

Congratulations! You've chosen a framework!

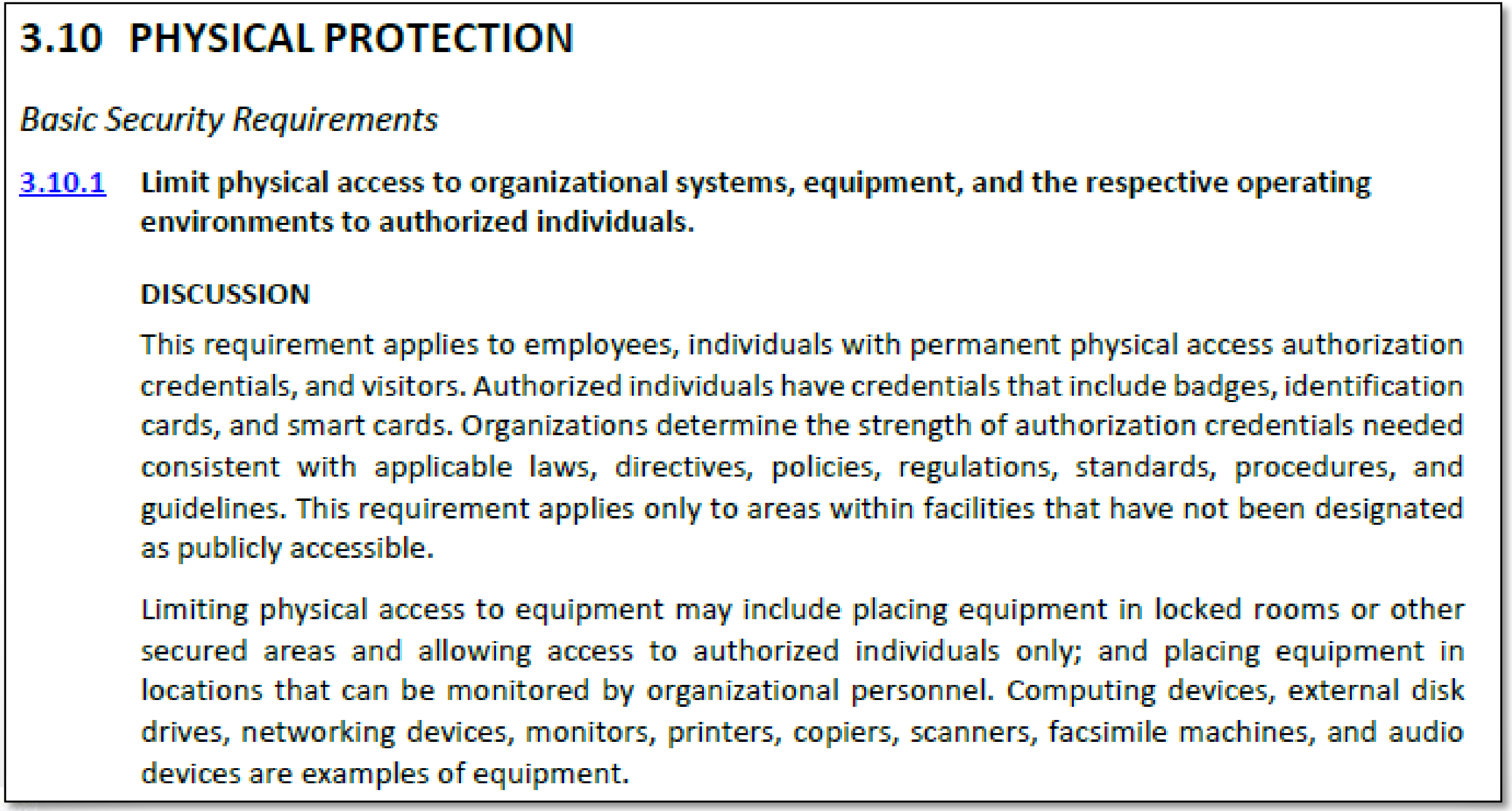
PUBLIC
CONTRACTING
INSTITUTE

Now the Journey Begins

Public Contracting Institute

Implementing NIST SP 800-171

How do you Prove Implementation of a Flexible Requirement?



3.10 PHYSICAL PROTECTION

Basic Security Requirements

3.10.1 **Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.**

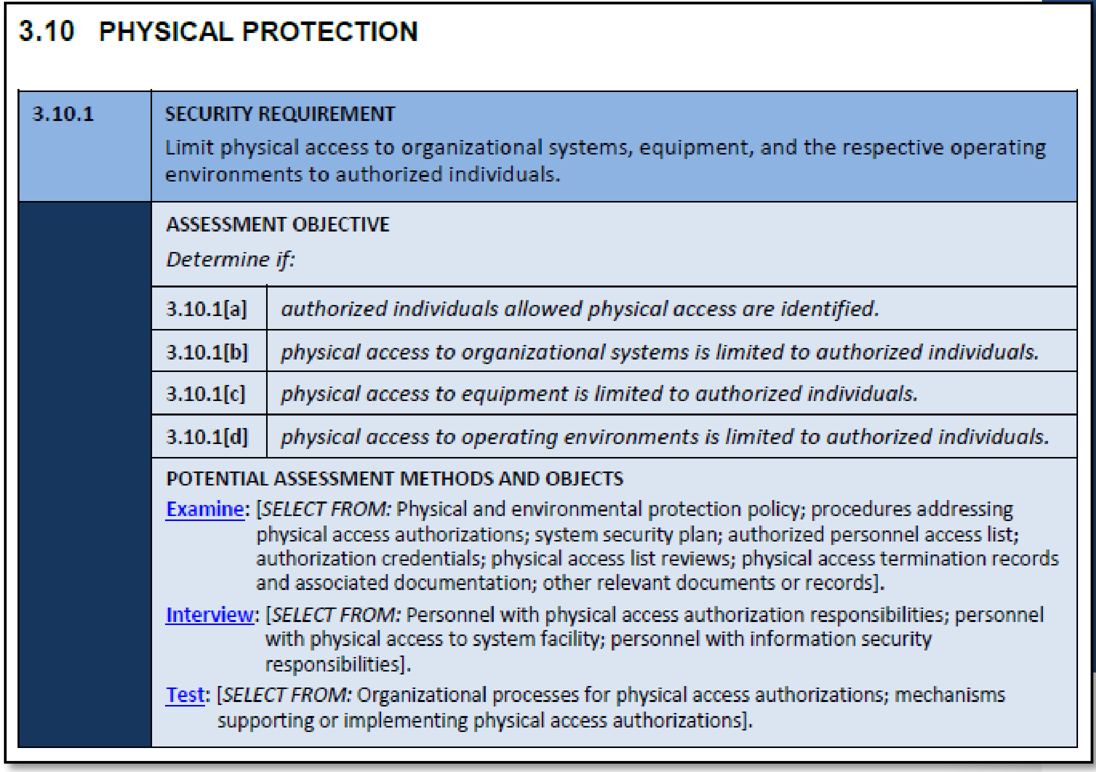
DISCUSSION

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

NIST SP 800-171A

- Assessment guide for NIST SP 800-171
- Defines a set of one or more “objectives” for each requirement (320 outcomes in total)
- Contractors still have flexibility when deciding how best to meet those objectives.



3.10 PHYSICAL PROTECTION

3.10.1	SECURITY REQUIREMENT Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.10.1[a]	*authorized individuals allowed physical access are identified.*
	3.10.1[b]	*physical access to organizational systems is limited to authorized individuals.*
	3.10.1[c]	*physical access to equipment is limited to authorized individuals.*
	3.10.1[d]	*physical access to operating environments is limited to authorized individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations].	

NIST SP 800-171

- Additional training for your staff is a smart investment.
- More than 50% of the requirements are non-technical.
- May force changes in business processes.
- Can take (at least) 12-18 months to go from 0 to fully implemented.

Public Contracting Institute

Meeting the NIST SP 800-171 Requirements

- You can outsource responsibility, but not accountability.
- Requires diligent selection of tools and services to ensure your service providers (e.g., cloud service providers, managed service providers) are doing their part to meet your compliance obligations.
- SMB adoption can cost $100,000+. Larger organizations likely to be higher.

Does Your Program Measure Up?

- Inventory your sensitive information to understand any additional legal and regulatory requirements
- Create an inventory of the people, practices, technology, and locations that are involved in the storing, processing, transmitting, or accessing of the sensitive information
- Evaluate that "inventory" against the requirements and objectives
- Create plans of action and milestones ("POA&Ms") for remediating any gaps that you identify
- Diligently work to close those gaps.

Critical POA&M Attributes

- Identification of the weakness/deficiency
- Plan of Action – a description of how you intend to remediate the deficiency
- Milestone(s), including expected completion date
- Resources needed for implementation
  - Criticality/Impact
  - Cost
  - Effort
  - People/points of contact
- Status

See: OMB Memorandum M-02-09

Remediation - Planning

- Create a remediation plan
- Group individual POA&Ms into projects
  - Related by subject matter area (“family”)
  - Related by type
    - Executive
    - Technical
    - Physical
  - Related by severity
  - Related by some combined metric
    - Impact/severity, effort, cost
- Prioritize your projects
  - Put your high impact/severity, low effort, low cost POA&Ms together and knock them out first(ish)
- Take action

Remediation - Execution

- Remediation can be a LONG process
- 12-18 months (or more)
- Requires culture change
- Must be driven from the top to be successful
- Can’t stop until all the gaps are remediated

Congratulations!
You’ve implemented a “reasonable” program!

PUBLIC CONTRACTING INSTITUTE

Right?

Unfortunately, no.

The CMMC Program

Should “Reasonableness” be Determined by Trust?

- DoD tried this in 2017
  - Added a contract clause (DFARS 252.204-7012) requiring that all contractors who handle CUI implement the requirements in NIST SP 800-171
- In the intervening 5 years, DoD has learned that either:
  - Contractors don’t read all of their contract clauses or
  - Contractors’ staff don’t truly understand the requirements or how to implement them
- Are you willing to trust your teams’ evaluation of their own work?
- Why should regulators, courts, or your clients trust you more than DoD’s contractors?

Reducing Inefficiencies and Taxpayer Burdens

- Trust alone isn't good enough.
- Spot-checking compliance is a numbers game and hasn't worked in the past.
- Whistleblowers aren't enough of a deterrent.
- The government doesn't have the resources to assess every government contractor's compliance.
- Asking contractors to fill out questionnaires for each contract is highly inefficient and time consuming for contractors and for the contracting officers, many of whom are not cyber experts. This approach would be extremely cost-prohibitive.
- You only find out that contractors' answers are "less than fully honest" after an incident. You can't put the cat back in the bag.
- DoD knew they needed to do something else to ensure compliance.

Cybersecurity Maturity Model Certification (“CMMC”) Program

- Embodied in 32 CFR 170 (proposed rule).
- Designed to ensure the government’s non-public information is properly safeguarded.
- Prior to contract award, (essentially) all contractors who handle CUI must obtain a CMMC certification.
- CMMC certification is a validation that the contractor has properly implemented the requirements in NIST SP 800-171.
- CMMC certification is issued for the contractor, not on a per-contract basis, improving efficiencies and reducing the cost to the government.

Who Issues the CMMC Certifications?

- Only ~3% of CMMC certifications will be issued by the government.
- Most CMMC certifications will be issued by commercial entities, called Certified 3rd Party Assessment Organizations (“C3PAO”).
- C3PAOs must adhere to ethical guidelines established by the CMMC Accreditation Body (the “Cyber AB”).
  - e.g., they cannot assess their own work
- C3PAOs employ specially trained, certified assessors to perform the CMMC assessments.
- C3PAOs can issue certifications to <u>any</u> organization, not just DoD contractors.

What does the Assessment Team Want to See?

In a word…

Evidence

Evidence Types

- **Examine** – Documentary evidence that describes the organization's business practices and how those practices enable the organization to meet all of the requirements/objectives.
- **Interview** – Discussions with the people who handle the implementation of the business practices to ensure what they do aligns with what is in the documentary evidence.
- **Test** – Shoulder surfing (or other evidence) that demonstrates that the organization is actually doing what is written in the documentation and what the staff said is being done.

Collecting and Organizing Your Evidence

- Assessors won’t accept a “data dump.”
- You need to do the diligence. The assessors are merely validating your assertion of compliance.
- Assessors expect to see a “traceability matrix” that shows how and where each piece of evidence is relevant for a given requirement/objective.
- Can be achieved in a number of ways, including:
  - Spreadsheets and File Folders
  - General Purpose Tools
  - Purpose-built Tools
- Look for:
  - NIST SP 800-171 **including NIST SP 800-171A objectives**
  - Creation and management of POA&Ms
  - Easy export of your information to common formats

Earn Your CMMC Certification

- Successfully demonstrate the adequate and sufficient implementation of all relevant requirements and objectives

While You're at it…

- Learn from DoD.
- Don't stop with your own program.
- Many cyber incidents are caused by authorized third-parties.
- Your organization does not operate in a vacuum; you have an entire supply chain.
- Making your vendors and service providers fill out extensive questionnaires is inefficient and expensive, both for you and them.
- Start asking your vendors and service providers for third-party certifications of their cyber programs, especially those who handle or have access to your sensitive information.

Summary

Demonstrating Reasonable Safeguarding of Sensitive Information

- Implement the requirements in NIST SP 800-171
- Perform a self-assessment using the objectives in NIST SP 800-171A
- Remediate any gaps you identify
- Collect evidence that demonstrates your compliance with the requirements
- Bring in a C3PAO to assess you and issue a CMMC certification
- Start asking for certifications from your suppliers and vendors who handle your sensitive information.

Public Contracting Institute

Thank You!

Please provide session feedback

CUI INFORMED

https://CUIInformed.com

FutureFeed

15 Minutes with FutureFeed:
https://FutureFeed.co/15