CONNSTEP
a CBIA affiliate

CMMC PREPARATION Webinars: Understanding CMMC Timeline & Steps to Compliance

CONNSTEP
3/9/2023

CMMC PREPARATION Webinars

Four Webinar Series

3/9 – 6/1

12 noon – 1 pm

March 9th	Understanding CMMC Timeline & Steps to Compliance
April 6th	How to Develop & Implement Effective CMMC Policies & Procedures
May 4th	How to Leverage Your IT Managed Service Provider (MSP) to Achieve CMMC Compliance
June 1st	Steps to Take in Preparation for a CMMC Audit

Webinar #1 Agenda

Understanding CMMC Timeline & Steps to Compliance:

1. Requirements CliffsNotes - the Who, What, How, and WHEN
2. CMMC Roll-out Update
3. Steps to Compliance
4. DCMA Assessments Findings
5. Success Factors and Resources

CONNSTEP
a CBIA affiliate

Presenters:

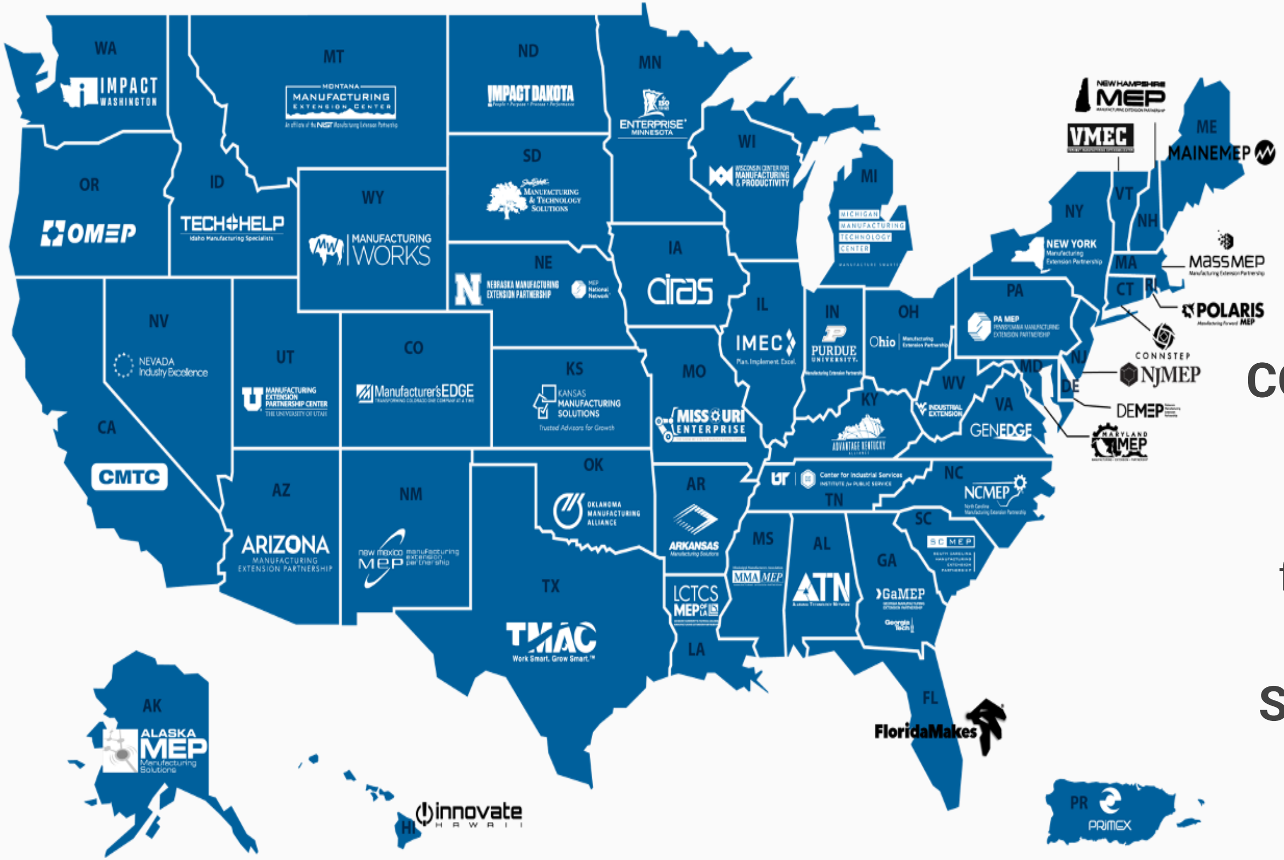
Anna Mumford
Cybersecurity Consultant

860.305.8880
amumford@connstep.org

Jeffrey Orszak
Director, Business Technology and Innovation

860.539.4905
jorszak@connstep.org

CONNSTEP is Connecticut's MEP


WA
IMPACT WASHINGTON
MT
MONTANA MANUFACTURING EXTENSION CENTER
ND
IMPACT DAKOTA
MN
ENTERPRISE MINNESOTA
OR
OMEP
ID
TECHHELP
Idaho Manufacturing Specialists
WY
MANUFACTURING WORKS
SD
South Dakota Manufacturing & Technology Solutions
WI
WISCONSIN CENTER FOR MANUFACTURING & PRODUCTIVITY
MI
MICHIGAN MANUFACTURING TECHNOLOGY CENTER
NE
NEBRASKA MANUFACTURING EXTENSION PARTNERSHIP
IA
ciras
NV
NEVADA Industry Excellence
UT
MANUFACTURING EXTENSION PARTNERSHIP CENTER
THE UNIVERSITY OF UTAH
CO
Manufacturer's EDGE
KS
KANSAS MANUFACTURING SOLUTIONS
Trusted Advisors for Growth
MO
MISSOURI ENTERPRISE
IL
IMEC
Plan. Implement. Excel.
IN
PURDUE UNIVERSITY
OH
Ohio Manufacturing Extension Partnership
PA
PA MEP
PENNSYLVANIA MANUFACTURING EXTENSION PARTNERSHIP
NY
NEW YORK Manufacturing Extension Partnership
VT
VMEC
NH
NEW HAMPSHIRE MEP
ME
MAINEMEP
MA
MassMEP
RI
POLARIS
CT
CONNSTEP
NJ
NJMEP
DE
DEMEP
MD
MARYLAND MEP
VA
GENEDGE
WV
INDUSTRIAL EXTENSION
KY
ADVANTAGE KENTUCKY ALLIANCE
CA
CMTC
AZ
ARIZONA MANUFACTURING EXTENSION PARTNERSHIP
NM
new mexico MEP manufacturing extension partnership
OK
OKLAHOMA MANUFACTURING ALLIANCE
AR
ARKANSAS Manufacturing Solutions
TN
UT Center for Industrial Services
NC
NCMEP
SC
SC MEP
TX
TMAC
Work Smart. Grow Smart.
LA
LCTCS MEP of LA
MS
MMA MEP
AL
ATN
GA
GaMEP
Georgia Tech
FL
FloridaMakes
AK
ALASKA MEP
Manufacturing Solutions
HI
innovate HAWAII
PR
PRIMEX

CONNSTEP is the Connecticut representative of the

MEP National Network™

facilitated and sponsored by

the **National Institute of Standards and Technology**

Value Delivered to Clients

CONNSTEP
a CBIA affiliate

$439 M
Retained Sales

$83 M
Increased Sales

$21 M
Cost & Investment Savings

$51 M
Increased Investments

2,036
New & Retained Jobs

2021 & 2022 | Independent survey results as reported by the National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP)

Guidance

Nothing in this presentation (written, spoken, expressed, or implied) is legal advice.

Nothing in this presentation (written, spoken, expressed or implied) should be construed as an endorsement of any solution, product, service, or methodology.

Poll

DFARS Regulations, its purpose, and timeline

2015: DFARS 252.204-**7012** Regulation

- *Who*: **ANYONE who works under a DoD contract**
- ***What:***
  - protect CUI residing on a contractor's systems
  - report CUI loss incidents to DoD
  - flow down the clause in subcontracts
- ***How:*** implement **NIST SP 800-171 (NIST: non-regulatory body)**
- ***When:*** compliant by Dec 2017 – wide non-compliance

Nov 2020: DoD Interim Rule

DFARS 252.204-**7019** - **NIST SP 800-171** self-assessment results -> SPRS database

DFARS 252.204-**7020** - DoD assessors can conduct **NIST SP 800-171** assessment

DFARS 252.204-**7021** - Implement **CMMC** and flow down to subcontractors

CURRENT DFARS Requirements

CURRENT DoD Contracts:

NIST SP 800-171 Framework -> 110 practices

- DFARS 252.204-**7012** – protect CUI, report incidents, and flow down requirements
- DFARS 252.204-**7019** - self-assessment scores into SPRS system
- DFARS 252.204-**7020** – DoD assessors can conduct NIST SP 800-171 compliance assessments

FUTURE DFARS Requirements

UPCOMING DoD Contracts:

DFARS 252.204-**7021** – CMMC anticipated start date **June 2023**

- **CMMC 2.0 model** - three progressively sophisticated levels depending on the **type of information the supplier handles**
  - ✓ Level 1 (Foundational -> 17 practices)
  - ✓ Level 2 (Advanced -> 110 practices) = NIST SP 800-171
  - ✓ Level 3 (Expert -> 110+ practices)
- May require third-party certification OR self-assessment, depending on the **type of information** and **acquisition priority**

CMMC 2.0 Roll-out Update

June 2019	CMMC program announced
February 2020	CMMC version 1.0 model released
November 2021	CMMC version 2.0 released in response to 850+ comments received
July 2022	Submitted for the rulemaking process (~9-24 months, going through a rigorous process of being vetted on the government side)
June 2023	Expected publication of the interim final rule
June - July 2023	60-day comment period
May 2023 and beyond	CMMC requirements could begin appearing in solicitations: • Phase 1 – self-assessments only (with an affirmation of compliance by a senior company official) • Phase 2 – self-assessments and 3rd party certifications (if required)
Late 2023 to early 2024	Publication of final rules.

https://www.governmentcontractslawblog.com/2022/06/articles/cybersecurity/updated-timeline-for-cmmc-implementation/ with updates

CMMC Roll-out Update

CMMC 2.0 Roll-out Update:

- The phased roll-out timeline can still change (take longer) - there will be recognition of previous assessments conducted
- During this time, the DoD encourages the DIB sector to strengthen its cybersecurity compliance posture:
  - performing a comprehensive self-assessment
  - remediate any gaps
  - update score to reflect the current posture
- DoD has announced it will be checking the accuracy of reported scores in SPRS by performing “medium assessments”
- Provision for requirements waivers – based on the government’s rapid need for company products **currently not in the DoD supply chain**

Prime Contractors Focusing on SPRS Scores

The Primes may still have their requirements for certification to mitigate their own risk:

- Primes need to manage their cyber risk
- Since there are no CMMC certifications available to help determine risk, they need to validate compliance by other mechanisms (e.g., SPRS score, assessments, surveys, etc.)
- Prime contractors have contractual responsibilities and must prepare their ENTIRE supply base
- They will be using this time to press forward on cyber compliance and determine which supplier will meet the requirements

What's at Stake?

Impact of a Security Attack on SMM

- Financial loss & operational downtime
- Reputation and image damage
- Loss of proprietary data and intellectual property
- Contractual and legal obligations
- Adopting Cybersecurity Framework protects CT organizations against punitive damage assessment for cybersecurity negligence

Actions to Take

1. Identify the data your company handles
2. Recognize customer-specific requirements
3. Flow down the DFARS requirements if you send CUI to your supply base
4. Submit your correct score to the SPRS

What to Expect

What to Expect while Embarking on Cybersecurity Journey?

- 6 to 18-month process
- Change of business processes, physical and operational protection controls, new procedures, documentation, companywide training programs
- Upgrading IT technologies and support
- Ongoing security risks assessment and management
- Develop a cadence for ongoing compliance maintenance
- Implementing a culture of change management, employee engagement, and collaboration

Steps to Becoming Compliant with DFARS

- Cybersecurity Gap Analysis
- Plan of Action and Milestones (POAM)
- System Security Plan
- *Enter score in SPRS Database*
- **Policies and Procedures**
- **Incident Response Plan**
- **Risk Management and Governance**

CMMC: evidence-based practices built into
the Business Structure that demonstrates security maturity

Policies and Procedures:

- Develop
- Document
- Implement
- Train
- Monitor
- Manage Risk
- Maintain

Human Errors lead to over 80% of all Security Incidents

Protection method?

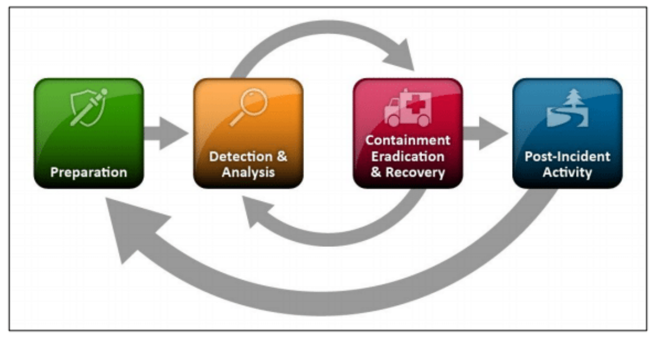
Acceptable Use Policies & Procedures

Security Incident Response

CONNSTEP
a CBIA affiliate

How to Build Security Incident Response Capabilities?

- Incident Response Plan
- Inter-departmental response team
- Communication plan
- PR strategy
- Team training exercises
- Lessons learned
- Relationships with external resources
- Cyber insurance
- Reporting requirements, etc.



Actions to Take

1. Develop a robust System Security Plan reflecting the current state
2. Identify POAM remediation plans with start/end dates, milestones, and action owners
3. Create an Incident Response Plan and internal team with roles and responsibilities

NIST SP 800-171 DCMA Scoring

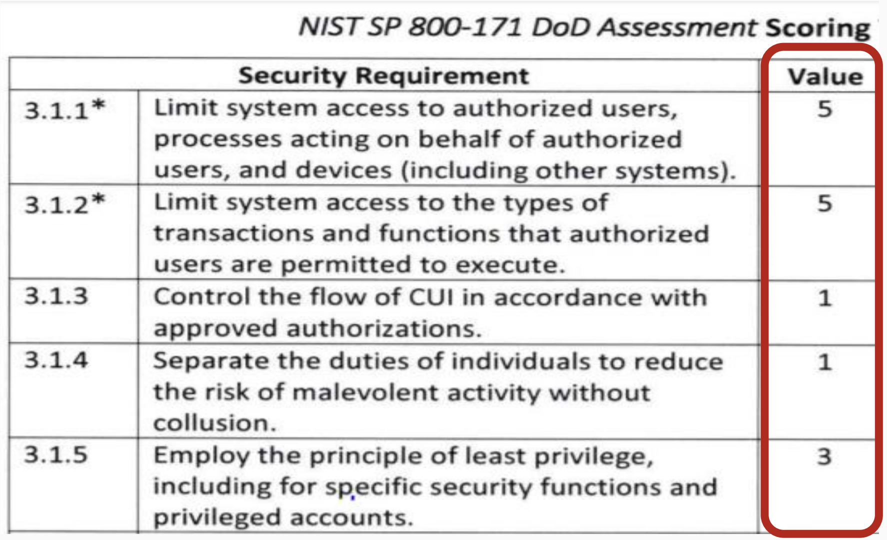
DCMA Scoring Methodology

- start at 110 points
- subtract 1, 3, or 5 points for each unimplemented requirement
- score range: -203 to 110

Submit the score to SPRS with an affirmation of compliance by a senior company official

No SSP: Noncompliance with DFARS 252.204-7012

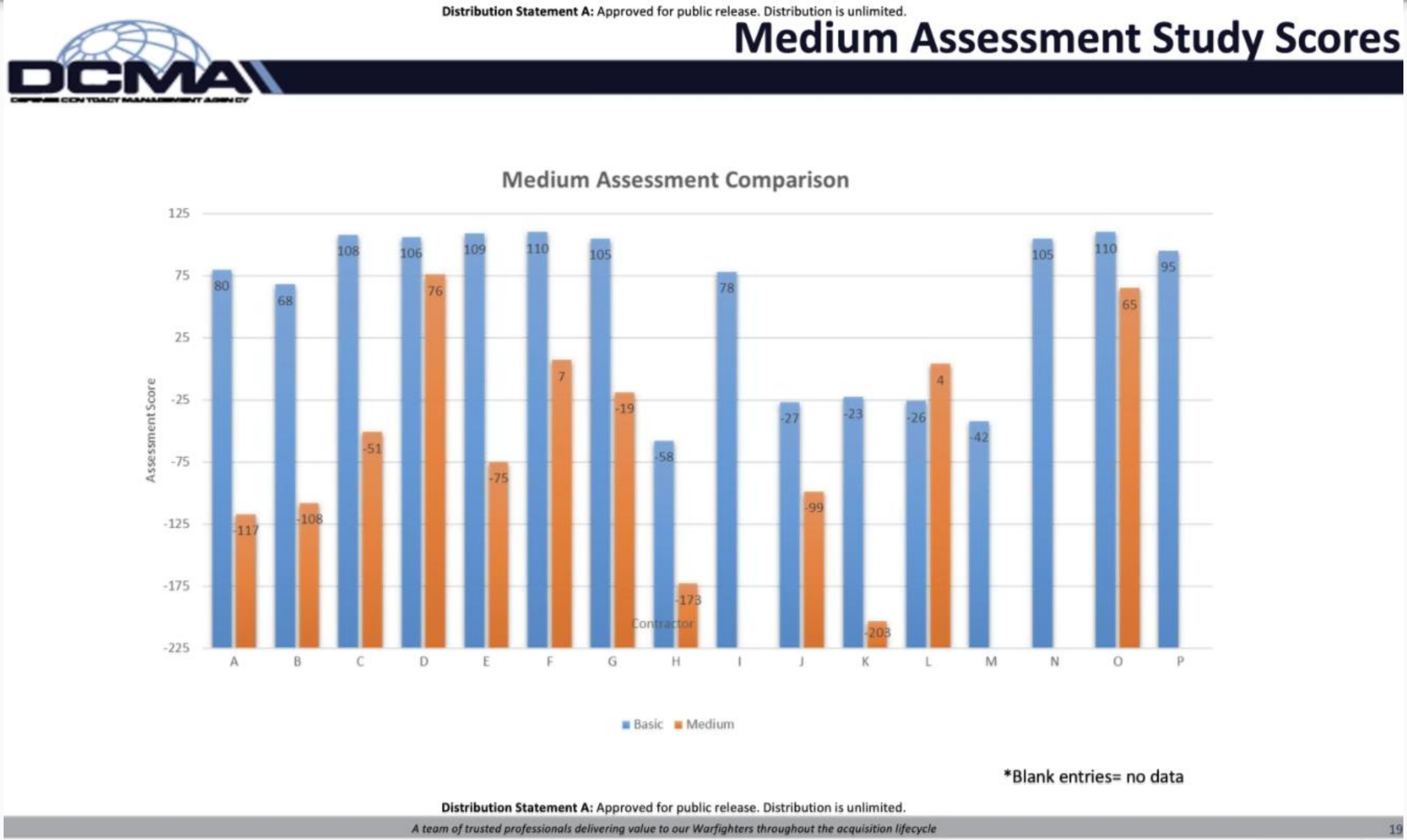
Not all requirements have equal weight



NIST SP 800-171 DoD Assessment **Scoring**

Security Requirement		Value
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3

DCMA Audit Assessments



Distribution Statement A: Approved for public release. Distribution is unlimited.

Medium Assessment Study Scores

DCMA
DEFENSE CONTRACT MANAGEMENT AGENCY

Medium Assessment Comparison

*Blank entries= no data

Distribution Statement A: Approved for public release. Distribution is unlimited.

A team of trusted professionals delivering value to our Warfighters throughout the acquisition lifecycle

19

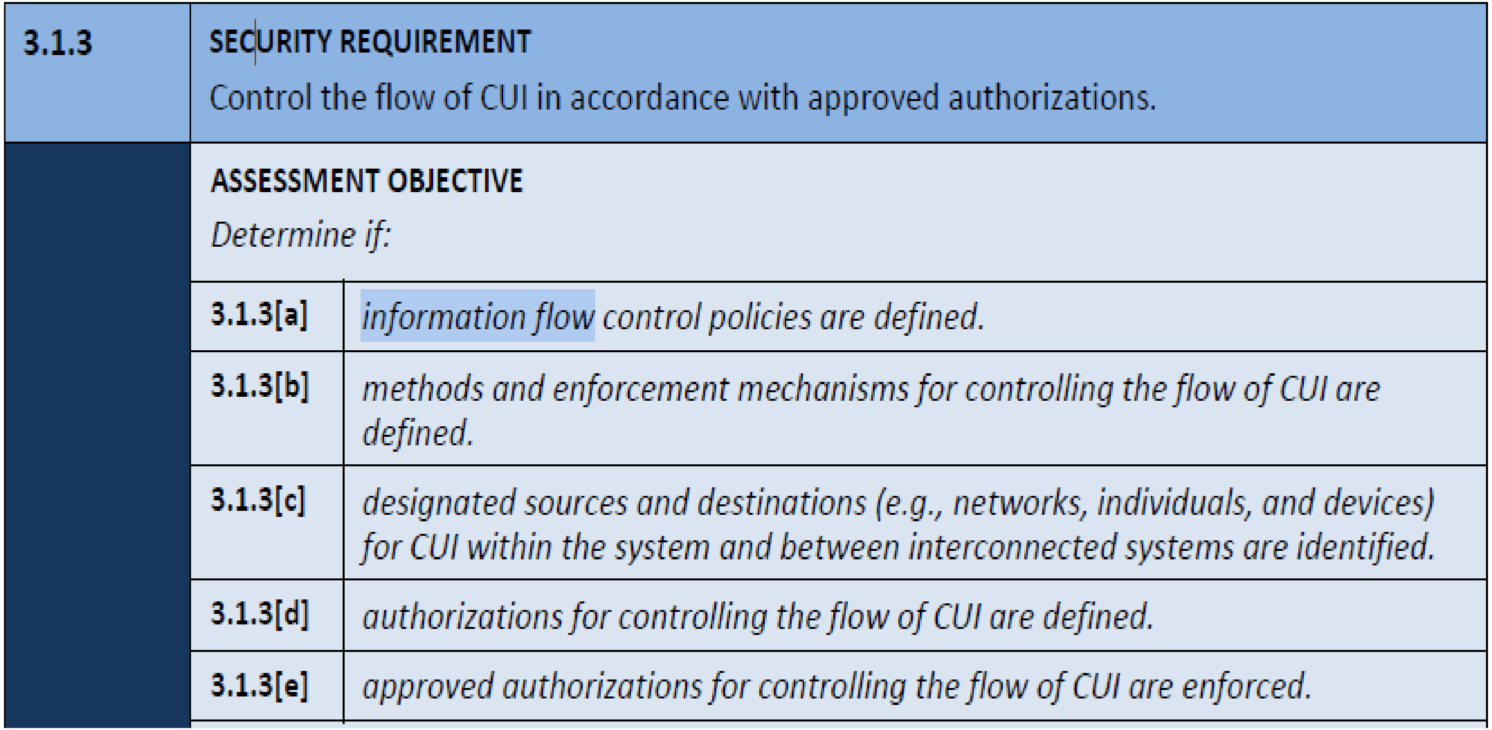
Medium Confidence Assessments

- DIBCAC has begun conducting Medium Confidence assessments on SMMs
- Reported SPRS scores widely overinflated
- Prosecuting intentional misrepresentations through their Civil Cyber Fraud Initiative within the DoJ

Key reasons for scores overinflation:

1. Not understanding requirements (depth and breadth of controls)
2. Failing to provide documentation and evidence

NIST SP 800-171A*



3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*

*NIST SP 800-171A is the assessors’ guide to the NIST SP 800-171 requirements

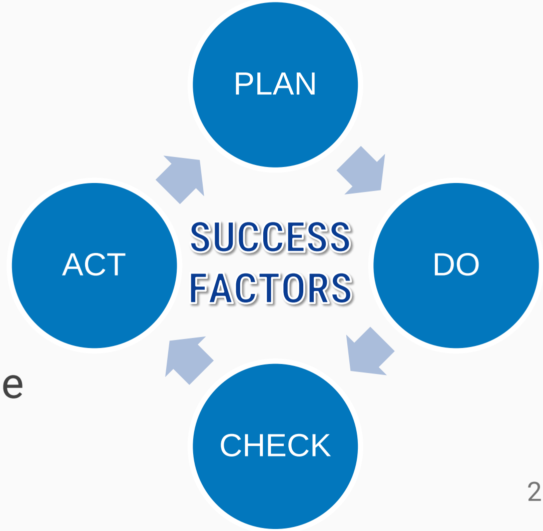
Actions to Take

1. Download NIST SP 800-171A (Assessors Guide)
   https://csrc.nist.gov/publications/detail/sp/800-171a/final
2. Download the CMMC Assessment Guide
   https://dodcio.defense.gov/CMMC/Documentation/
3. Become familiar with the objectives of each control (the depth and breadth of controls)

Success Factors

What Factors make Cybersecurity Programs Successful?

- Executive support and strategy
- Involved leadership overseeing security governance
- Dedicated team with business, operations, and procedural background
- Strong project manager
- Cost-effective, progressive business solutions
- Partnership with "the right" MSP and MSSP



Download: A Guide to Help SMMs Achieve Cybersecurity Compliance with the Right IT MSP Partner

https://bit.ly/msp-guide

President Biden is urging the industry to participate in the “Shields Up” campaign against Russian cyber aggression.

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.

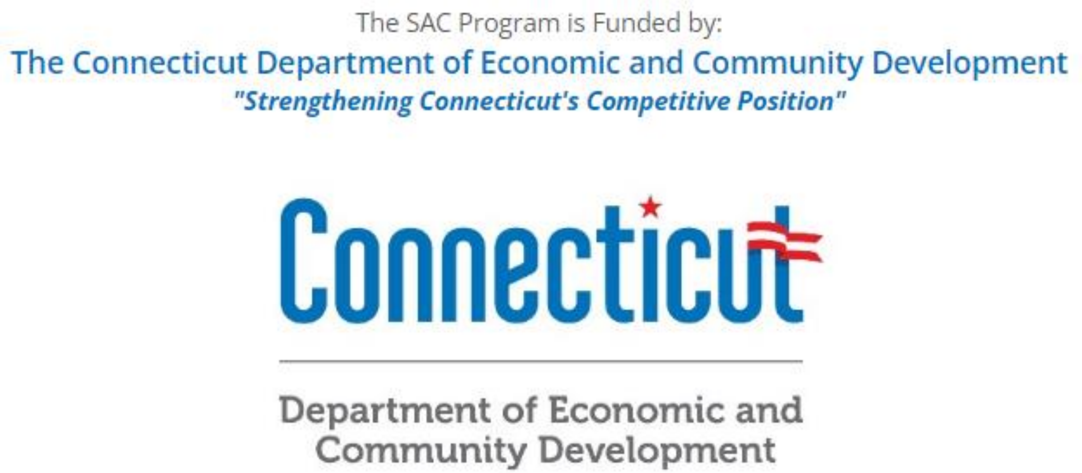
https://www.cisa.gov/shields-up

State Funding Available

State funding is available for

Connecticut Manufacturing SIRI and CYBER Assistance Program (SAC)

for manufacturing companies or allied service providers located in Connecticut.



The SAC Program is Funded by:

The Connecticut Department of Economic and Community Development

"Strengthening Connecticut's Competitive Position"

https://ctsac.ccat.us/

Questions?

Glossary

CMMC – Cybersecurity Maturity Model Certification
CUI - Controlled Unclassified Information
DFARS - Defense Federal Acquisition Regulation Supplement
DIB – Defense Industrial Base
DIBCAC – Defense Industrial Base Cybersecurity Assessment Center
DCMA – Defense Contract Management Agency
IRP – Incident Response Plan
IT – Information Technology
MEP - Hollings Manufacturing Extension Partnership
MSP – Managed Service Provider
MSSP – Managed Security Service Provider
NIST – National Institute of Standards and Technology
NIST SP 800-171 – NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
POAM – Plan of Action and Milestones
SPRS – Supplier Performance Risk System
SSP – System Security Plan

Questions and Answers

Q: We are a manufacturer of aerospace parts and migrating to Microsoft 365. Microsoft is stating we need a higher level (GCC High) of security than what our IT managed service provider thinks we need. What level is required?
A: To correctly protect CUI on Microsoft 365 that CUI needs to reside on a GCC High instance. Good data segregation practices can help reduce the number of instance needed.

Q: Who determines our priority and how do we know what priority our company has?
A: The priority will be determined by the DoD Program Officer for the Prime Contractor. As the Prime flows the information to sub-tiers, they could impose their own requirements.

Q: Are the DoD medium confidence assessments performed by DCMA?
Yes, by Defense Industrial Base Cybersecurity Assessment Center, which is part of DCMA.

Q: Has DCMA performed any assessments to date in Connecticut?
While we do not know the specific companies or geographics areas covered by DCMA audits, it is reasonable to believe Connecticut companies are included.

Q: Is funding available in Massachusetts that you know of?
We are aware that funding has been available in Massachusetts. You can contact MassMEP, massmep.org, to get current information on programs in Massachusetts.

Questions and Answers

Q: Should we capture the hours spent on the effort to become compliant?
A: We are not aware of any requirement to document the time that a company has spent becoming compliant. The CMMC will look for evidence that the controls for each requirement are being met.

Q: Does Connecticut offer any funding?
A: Yes, the Manufacturing Innovation Fund has several programs that could assist Connecticut companies in cybersecurity implementation. More information can be found at: https://www.ccat.us/programs/

Q: Some of the requirements are not explicit enough. For example, do we need something like ThreatLocker for blacklisting and whitelisting software or is it acceptable to just not be an admin on any workstation?
A: Each company should take a risk management approach to implement solutions that fit their business needs. CONNSTEP can provide advice on specific requirements.

Q: Will you be talking about how to identify and/or Mark CUI? Are there different handling requirements for CUI/CDI
A: We will add this to the agenda for the second session.

Q: Does CONNSTEP provide a Service to participate with a company for a DCMA audit?
A: CONNSTEP has not been as to participate with a company during a DCMA audit. We do offer a medium confidence gap assessment to help prepare for a DCMA audit.