Roadmap to Security

Who am I?

Matt Hoeper, CISSP, PMP
CISO at Winsor Consulting
mhoeper@winsorgroup.com
www.winsorconsulting.com

I can teach you about CMMC, I help you identify gaps in your organization, and I can recommend solutions.

I cannot certify you.

What is CMMC?

- CMMC stands for “Cybersecurity Maturity Model Certification”
- Version 1.02 was released on 3/20/20
- Includes 5 levels that range from "Basic Cybersecurity Hygiene" to "Advanced"
- The required minimum level to be listed on the RFP and used as a "go/no go decision"
- EVERY company performing work for the DoD or supply chain will be required to comply, even companies that do not handle CUI will require Level 1

How About Some Definitions?

- CUI (Controlled Unclassified Information) is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.
  - CUI *is not* classified information. It is *not* corporate intellectual property unless created for or included in requirements related to a government contract.
- FCI (Federal Contract Information) is information provided by or generated for the Government under contract not intended for public release.
- Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government. But, while FCI is any information that is “not intended for public release,” CUI is information that requires safeguarding.

All CUI in possession of a government contract is FCI but not all FCI is CUI.

LEVEL 1
BASIC CYBER HYGIENE

17 PRACTICES

- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE

72 PRACTICES

- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE

130 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE

156 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

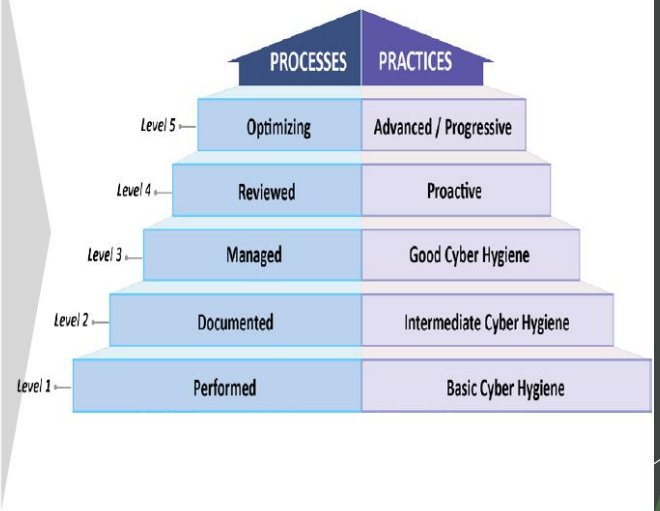
LEVEL 5
ADVANCED / PROGRESSIVE

171 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

The Whole Maturity Model

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	



The 10 Controls

1. AC.1.003 – Controlling limiting connections
2. IA.1.076 – Authentication
3. PE.1.131 – Physical access to systems
4. PE.1.132 – Visitor escorting and logging
5. AU.2.044 – Reviewing audit logs
6. MP.2.121 – Removable media
7. RE.2.137 – Backups (performing and testing)
8. IA.3.083 – Multifactor authentication
9. IR.2.092 – IR planning
10. RM.3.146 – Risk mitigation plans

The Approach

- Read the control. What does it say?
- What does it mean? Do the research. What is trying to be accomplished?
- Letter of the law vs. spirit of the law.
- How do I apply it to our organization?
- Policies vs. Procedures. We need to PROVE we're doing it.

Control 1 - AC.1.003

What does it say?

"Verify and control/limit connections to and use of external information systems."

What does it mean?

Control/manage connections between your company network and outside networks. Organizational resources should be used for organizational tasks.

How do I apply it?

Implement a policy/procedure to control/manage network connections, as well as limiting personal devices from accessing company networks and information.

How do I prove it?

Policy, technical configuration.

Control 2 - IA.1.076

What does it say?

"Identify information system users, processes acting on behalf of users, or devices."

What does it mean?

Make sure to assign individual, unique identifiers (e.g., user names) to all users and processes that access company systems.

How do I apply it?

Do not use shared accounts. Know who/what is logging in. Always use unique identifiers.

How do I prove it?

Policy, technical configuration (like Active Directory).

Clarification - IAAA

Identification

Authentication

Authorization

Accountability (Auditing)

Control 3 - PE.1.131

What does it say?

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

What does it mean?

Designate public and private areas within the organization, where devices are only accessible to authorized personnel.

How do I apply it?

For those parts of your company to which you want only specific employees to have physical access, monitor or limit who can enter those spaces with badges, key cards, etc.

How do I prove it?

Physical access control policy, lists of personnel with authorized access, special designations for sensitive parts of the facility.

Control 4 - PE.1.132

What does it say?

"Escort visitors and monitor visitor activity."

What does it mean?

Escort visitors and monitor visitor activity.

How do I apply it?

Do not allow visitors, even those people you know well, to walk around your facility without an escort. Make sure that all non-employees wear special visitor badges and/or are always escorted by an employee while on your property.

How do I prove it?

Policy, temporary badge system.

Control 5 – AU.2.044

What does it say?

"Review audit logs."

What does it mean?

Review audit logs.

How do I apply it?

Ensure that you review your audit logs. Logs should be checked regularly.

How do I prove it?

Policy and procedure for reviewing logs. Maybe a software solution.

Control 6 – MP.2.121

What does it say?

"Control the use of removable media on system components."

What does it mean?

Any type of media storage that you can remove from your computer needs to be controlled: CDs, DVDs, USB drives.

How do I apply it?

Limit the use of removable media to the smallest number needed. Scan all removable media for viruses. Track removable media that you own and make sure you reuse and dispose of it properly.

How do I prove it?

Policy, technical configuration.

Control 7 – RE.2.137

What does it say?

"Regularly perform and test data backups."

What does it mean?

Regularly back up your data so you can recover it if there's a hardware or software failure. Test the backups.

How do I apply it?

Schedule backups to run automatically or manually and then test it on a regular basis.

How do I prove it?

Have a defined backup strategy with procedures showing how you back up data, where you store it and how you test it.

Control 8 – IA.3.083

What does it say?

"Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts."

What does it mean?

Passwords alone aren't enough. Another authentication factor is needed in many cases.

How do I apply it?

Implement an MFA solution for accounts that have elevated access and for outside network access.

How do I prove it?

MFA technical configurations.

Control 9 – IR.2.092

What does it say?

"Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities."

What does it mean?

Have an incident response plan.

How do I apply it?

Develop an incident response plan.

How do I prove it?

The IR plan.

Control 10 – RM.3.146

What does it say?

"Develop and implement risk mitigation plans."

What does it mean?

You'll need a strategy for mitigating risk.

How do I apply it?

Identify risks and have a response to each one.

How do I prove it?

The risk mitigation plan.

How can we help?

Matt Hoeper, CISSP, PMP
CISO at Winsor Consulting
mhoeper@winsorgroup.com
www.winsorconsulting.com

This can be a daunting task. Don't go it alone.

Emily Lee will provide a copy of the slides from this presentation.