Playbook FOR CMMC 2.0 Level 1

The Digital Manufacturing
& Cybersecurity Institute

The Digital Manufacturing
& Cybersecurity Institute

Playbook FOR CMMC 2.0 Level 1

CONTACT:

Laura Élan
Senior Director of Cybersecurity
laura.elan@mxdusa.org

Cesar Pena
Senior Cybersecurity Engineer
cesar.pena@mxdusa.org

MxD 1415 North Cherry Ave, Chicago, IL 60642
www.mxdusa.org

Introduction

Manufacturers and their suppliers who have, or hope to have, contracts with the U.S. Department of Defense must soon meet new cybersecurity requirements. This MxD Playbook for Level 1 of the Cybersecurity Maturity Model Certification — or CMMC 2.0 — is designed to help you do that.

Level 1 is the first or foundational tier of CMMC 2.0's three levels. It has 17 security practices to master and requires an annual self-assessment. It's designed to protect Federal Contract Information (FCI) received by and shared with contractors and subcontractors.

With this Playbook, MxD delivers a quick-start guide for Level 1, labeling the security practices by degree of difficulty; clarifying instructions; and providing tips from lessons we learned as we implemented these same security practices. A glossary defines some of the terms you will come across as you navigate this process and includes a link to the full National Institute of Standards and Technology (NIST) list of cybersecurity words and acronyms.

For manufacturers just starting with CMMC 2.0, MxD recommends looking first at the security practices labeled "easy." Most organizations will find that they already are implementing at least a portion of them. As you continue on your path, tackle security practices we have identified as "medium," turning last to those labeled "hard."

MxD, the nation's digital manufacturing institute and National Center for Cybersecurity in Manufacturing, is committed to preparing manufacturers to compete in the decades to come. Enhanced cyber protection is key to that preparation. This Playbook, which complements the MxD Cyber Marketplace, will help you get started.

Contents

DOMAIN: ACCESS CONTROL

DOMAIN: IDENTIFICATION AND AUTHENTICATION

DOMAIN: MEDIA PROTECTION

DOMAIN: PHYSICAL PROTECTION

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION

DOMAIN: SYSTEM AND INFORMATION INTEGRITY

Glossary

NIST provides an extensive glossary of security terms at https://csrc.nist.gov/glossary/. Some of those terms, with definitions including from NIST and other federal government sources, are listed here:

Application allowlisting: A security technique that permits only specific software applications or functions to run on a system.

Auditable: Able to be audited, meaning there is a record available for review by a third-party to confirm that a requirement is met.

Authenticate: Verifying the identity of a user, process, or device before allowing access to resources in an information system.

Authorize: Confirming that a user, process, or device is allowed to access a system resource.

Confidential information: Material that should not be disclosed, viewed, or accessed by unauthorized people or processes.

Control: Any process, policy, device, practice, or other action that modifies or manages cybersecurity risk. Terms used interchangeably are security capability and security practice.

Cryptographic device: A physical device that can perform functions including encryption, which converts information so that it is not easily read by a human or a machine.

Federal contract information (FCI): Information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments.

Malware: Software or firmware that aims to perform an unauthorized process that will adversely impact the confidentiality, integrity, or availability of a system.

Multi-factor authentication: Use of two or more factors to verify identity. Factors include “something you know,” such as a password or PIN; “something you have,” such as a token; or “something you are,” such as a fingerprint or facial recognition.

Patch: A fix, or immediate solution, to an identified problem. It can sometimes be downloaded from a software-maker’s website.

Phishing: Use of deceptive computer-based means to trick individuals into disclosing sensitive information.

Tampering: An intentional, unauthorized action that results in modification of a system, its components, its intended behavior, or data.

Threat: A potential cause — including cybercriminals — of an unwanted incident that may lead to the harming of a person, system, or organization.

Vulnerability: Weakness in a system, system security procedures, internal controls, or implementation that a threat could exploit or trigger.

DOMAIN: ACCESS CONTROL

AC.L1-3.1.1

Authorized Access Control

DEGREE OF DIFFICULTY: EASY [✓ MEDIUM] HARD

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

WHAT: Put policies in place to control access between subjects (like users or processes) and objects (like devices, files, or printers).

HOW: Identify which users and processes need access to hardware, software, and data on your information technology (IT) networks. Users may be employees or guests or suppliers and vendors who interact directly with the company's information, hardware, or data systems. Processes include such functions as automatic software updates that act on behalf of administrators and users.

Set up systems so that only authorized users and devices are allowed and limit the devices that can be accessed by company computers. Maintain a list of all authorized personnel.

MxD'S ADVICE / LESSONS LEARNED

- Require a username and password login for each employee entering the network.
- After a person logs in, determine access based on their job and the information they need to do it.
- Add security with multi-factor authentication, which asks employees to confirm their identities with steps such as a popup code on their phone.
- Make sure employees choose strong passwords and update them regularly.
- Reinforce good security practices with training.
- Choose as many different mechanisms as possible to ensure that only authorized people, equipment, and processes are allowed onto network resources. It's like Swiss cheese: There are holes in all the layers, but stacked up they provide enough protection.

IN DETAIL

At MxD we had the ability to easily connect devices to our network. During our CMMC Level 1 review, we realized it was too easy. What made connection easy for our employees also made it easy for bad actors to connect to our network. We decided to clamp down. We made sure only certain devices are allowed to connect to the network at a designated physical port. If one of us now tries to connect a laptop at a coworker's desk, access to the network is blocked.

DOMAIN: ACCESS CONTROL

AC.L1-3.1.2

Transaction and Function Control

DEGREE OF DIFFICULTY: EASY [✓ MEDIUM] HARD

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

WHAT: Spell out what authorized users are allowed to do on the company networks. Limit system access to the transactions and functions that are defined for each user.

HOW: Choose who gets what access based on their department; whether they are an employee, guest, or vendor; or if they will be on networks temporarily or permanently. For example, only workers in human resources need access to payroll data.

MxD'S ADVICE / LESSONS LEARNED

- Install control mechanisms like encryption so confidential information can be accessed by only those workers who need it to do their jobs.
- Limit what those with access can do, such as read, edit, or delete files or information. FCI is like payroll data — only certain employees should be able to access it.

DOMAIN: ACCESS CONTROL

AC.L1-3.1.20

External Connections

DEGREE OF DIFFICULTY: EASY **MEDIUM** HARD

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

WHAT: Check if the connections to, and use of, external systems are identified, verified, and limited.

HOW: Restrict connections from external devices to your company networks. These include employees' personal cell phones or a personal laptop that someone might use at home to work on a company project.

MxD'S ADVICE / LESSONS LEARNED

- Allow only company-issued devices to access your corporate network, specific files, and confidential information.
- Use a guest Wi-Fi network as one way to keep external devices — including those belonging to staff or visitors — off the corporate network.

DOMAIN: ACCESS CONTROL

AC.L1-3.1.22

Control Public Information

DEGREE OF DIFFICULTY: [✓ EASY] MEDIUM HARD

Control information posted or processed on publicly accessible information systems.

WHAT: Have a system in place to ensure that confidential FCI is not posted where the public can see it, like on the company website.

HOW: Review everything related to federal contracts before it is posted on any publicly accessible spot. Limit who is authorized to post and ensure that systems are in place to immediately remove any confidential information that accidentally becomes public.

MxD'S ADVICE / LESSONS LEARNED

- As stated before, remember that FCI is like payroll data — only certain employees should see it.
- Restrict posting capability to a dedicated person or team, like the communications staff.

DOMAIN: IDENTIFICATION AND AUTHENTICATION

IA.L1-3.5.1

Identification

DEGREE OF DIFFICULTY: EASY [✓ MEDIUM] HARD

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

WHAT: Make sure you can identify who and what are accessing your company networks.

HOW: Assign employees unique usernames. There are many technical ways to track the source of any information on a network, including the use of media access control (MAC) or internet protocol (IP) addresses.

MxD'S ADVICE / LESSONS LEARNED

- Ensure that you know all allowed hardware and software.
- Monitor network traffic to detect hardware or software not on that list. Third-party service providers are a great way to accomplish this.

DOMAIN: IDENTIFICATION AND AUTHENTICATION

IA.L1-3.5.2

Authentication

DEGREE OF DIFFICULTY: EASY **MEDIUM** HARD

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

WHAT: Be certain that all users — people and devices — are authenticated or verified before they can access your systems.

HOW: Assign passwords (the most common way to do this). Other authenticators include keycards, biometric sensors including fingerprint scanners, or keypads.

MxD'S ADVICE / LESSONS LEARNED

- Understand that one of the easiest ways a security incident can happen is if usernames and passwords for employees or equipment are not unique and updated.
- Have employees change default passwords immediately after receiving initial login information and do so again at regular intervals.
- Make sure to change default passwords when you attach new equipment to the network. This is crucial because default login information is easy to find on the internet. Then it can be used to compromise a company or security system.
- Test and train to make sure employees are not using default login information.

IN DETAIL

MxD implemented single sign-on (SSO), which allows a person to use a single password to sign in once to access multiple business applications. SSO encourages users to create one strong password as opposed to several weaker passwords that must be memorized or even written down – security risk! SSO is a great convenience, but it also has risks; if a username and password are compromised, then all the systems tied to the SSO may be compromised. To add protection, MxD added multi-factor authentication for all systems tied to SSO. The authentication has a time-out mechanism so it must be reaffirmed.

DOMAIN: MEDIA PROTECTION

MP.L1-3.8.3

Media Disposal

DEGREE OF DIFFICULTY: **EASY** MEDIUM HARD

Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

WHAT: Destroy or wipe clean any tools that include FCI (digital or non-digital) before they are thrown away or reused. These can include laptop computers, cell phones, scanners, copiers, and even papers left at workstations. This ensures that sensitive information is not accidentally shared when these items are used by someone else.

HOW: Shred or destroy papers, CDs, or disk drives so they cannot be read after they are thrown away. Delete the contents of cell phones and any electronic devices before they are reused.

MxD'S ADVICE / LESSONS LEARNED

- Destruction is the best protection. If you have paper contracts, shred them and lock up the remains until they can be taken to a disposal facility.
- Break DVDs. Don't just throw these items into the trash.
- Delete sensitive information or remove hard drives or SIM cards before laptops or phones are sent out for repair.

IN DETAIL

MxD had good media disposal procedures for paper and DVDs, however we noticed we were not treating our hard drives the same way. We've now updated our procedures to ensure that any equipment sent out for repair or maintenance has no data files, information, or credentials. The easiest way to do this is removing the hard drive. When equipment returns, the hard drive is reinstalled.

DOMAIN: PHYSICAL PROTECTION

PE.L1-3.10.1

Limit Physical Access

DEGREE OF DIFFICULTY: **EASY** MEDIUM HARD

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

WHAT: Know who has access to different work areas, equipment, and information systems in your organization and limit that access to authorized workers.

HOW: Allow only authorized workers to access restricted office space, equipment, and organizational systems. Issue credentials including badges, identification cards, or smart cards that an employee must present to enter restricted work spaces. Place office equipment — such as computers, disk drives, and printers — in locked rooms or under staff supervision, ensuring only authorized workers can use it.

MxD'S ADVICE / LESSONS LEARNED

- Know that it's okay if parts of your organization are open to the public. You might have conference rooms where you host meetings, or a guest Wi-Fi network where visitors can log on.
- But draw your boundaries on a map, indicating where visitors can and can't go.
- Install turnstiles so that a badge must be swiped to enter sensitive areas of the building.
- Require workers to badge in and badge out daily so the company has a log of the comings and goings of those with access to FCI.

IN DETAIL

MxD initially believed that this security control would be easy to implement and that we had the right practices and policies in place. Those included badges and turnstiles that record when employees enter as well as internal door locks that limit building access. However, we determined early in our Level 1 compliance journey that though we had entry controls, we did not have a way to distinguish different types of guests. Another "aha" moment was that we tracked entries but not all exits. We now have an electronic system that records all entries and exits for each type of person entering our facility: employees, members, vendors, and visitors. We also learned that a logging system isn't sufficient. Physical access must be continually monitored. Therefore, our physical access mechanisms are supported by cameras, door alarms, and daily visual audits.

DOMAIN: PHYSICAL PROTECTION

PE.L1-3.10.3

Escort Visitors

DEGREE OF DIFFICULTY: [✓ EASY] MEDIUM HARD

Escort visitors and monitor visitor activity.

WHAT: Ensure that all visitors are escorted by an employee for the entire time they are on-site.

HOW: Give visitors badges identifying them as guests before they enter the secure part of the building. Encourage employees to approach unaccompanied guests and connect those visitors with staff members who can escort them.

MxD'S ADVICE / LESSONS LEARNED

- Don't let visitors walk around the facility freely.
- Consider providing guests with lanyards or badges that are a different color than employees' so they are easily identifiable.
- Provide visitor guides that explain rules, like staying with escorts while on-site and not taking photos or videos beyond certain security boundaries.

DOMAIN: PHYSICAL PROTECTION

PE.L1-3.10.4

Physical Access Logs

DEGREE OF DIFFICULTY: [✓ EASY] MEDIUM HARD

Maintain audit logs of physical access.

WHAT: Keep a record of everyone who accesses any part of your facility.

HOW: Have employees and guests sign in and out. That can be done on a sheet of paper or via electronic means like on a tablet or with badge readers. Determine how long those records should be kept.

MxD'S ADVICE / LESSONS LEARNED

- Keep auditable logs of who comes and goes. Keeping those paper copies or electronic records is important.
- Make sure to record when people leave, too. That step is often forgotten and you don't want an unescorted visitor in the building after everyone else is gone.
- Check contracts to see if they stipulate how long such records must be kept.

DOMAIN: PHYSICAL PROTECTION

PE.L1-3.10.5

Manage Physical Access

DEGREE OF DIFFICULTY: EASY MEDIUM HARD

Control and manage physical access devices.

WHAT: Make sure you know who is physically able to access your business and the different areas within it whether by key, badge, or keycard.

HOW: Do this manually or electronically. Track who is assigned what key or badge, and update that information as employees leave or change departments.

MxD'S ADVICE / LESSONS LEARNED

- Keep a list of how many keys you have for rooms like server or maintenance rooms — and who has them.
- Remember, if you have a combination lock on a storage cabinet, write down who has the combination.
- Track by keeping a list on paper or maintaining a computer spreadsheet.

©2022 MxD, The Digital Manufacturing Institute

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION

SC.L1-3.13.1

Boundary Protection

DEGREE OF DIFFICULTY: EASY MEDIUM [✓ HARD]

Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

WHAT: Define external and internal system boundaries. Monitor, control, and protect communications at these boundaries.

HOW: Use tools that include firewalls and routers at the connection points, or boundaries, where your network links to an external network (like the internet). Also, identify and protect at internal boundaries, such as the division between visitor and company Wi-Fi networks.

MxD'S ADVICE / LESSONS LEARNED

- Draw a diagram to figure out how information flows into and out of your organization.
- Use that picture to help you see where boundaries are, how devices are connected, and where you need to pay closer attention to the flow of data and communication.

©2022 MxD, The Digital Manufacturing Institute

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION

SC.L1-3.13.5

Public-Access System Separation

DEGREE OF DIFFICULTY: EASY MEDIUM [✓ HARD]

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

WHAT: Use subnetting to divide, or segment, a network. This will keep security vulnerabilities on one subnetwork from adversely impacting others.

HOW: Allow members of the public (like a visitor with a laptop) to access certain company resources, while preventing access to the full system by using subnetworks. These subnetworks, which are also called demilitarized zones, or DMZs, are typically defended with routers, gateways, and firewalls.

MxD'S ADVICE / LESSONS LEARNED

- Be aware that many companies have stopped relying on DMZs and now use cloud-based systems to host public information — such as job applications — and to separate that information from their own networks.
- Ensure these cloud environments, or similar subnetworks, have security protections.
- Don't just rely on the cloud service provider for security. It's a company's responsibility to keep data safe.

DOMAIN: SYSTEM AND INFORMATION INTEGRITY

SI.L1-3.14.1

Flaw Remediation

DEGREE OF DIFFICULTY: EASY MEDIUM HARD

Identify, report, and correct information and information system flaws in a timely manner.

WHAT: Specify the time frame in which you expect to have any security threats identified, reported, or fixed and ensure that you have processes in place to hit those deadlines.

HOW: Identify which systems might be affected by software and firmware flaws as well as those with any potential vulnerabilities. Make sure all security updates are installed right away. These could include patches, service packs, hot fixes, and anti-virus signatures.

MxD'S ADVICE / LESSONS LEARNED

- Patch, patch, patch and train employees so that if they see something, they say something. Workers often know about vulnerabilities yet don't flag or fix them right away. That's like leaving a door unlocked.
- Keep in mind that failing to patch is a big security risk.
- Plan to install system patches when doing routine maintenance to minimize downtime.
- Check the national vulnerability database (**https://nvd.nist.gov/**). It ranks vulnerabilities, scoring them from zero to 10, with 10 the most crucial to fix. Don't ignore severe vulnerabilities.
- Work with equipment vendors to guarantee you are getting alerts about flaws or needed patches. Update alerts are routine in the information technology (IT) world, but not always the case with operational technology (OT).
- If you outsource security operations, make sure the contract with the provider defines the required speed of reporting of and updates to identified system flaws.

©2022 MxD, The Digital Manufacturing Institute

DOMAIN: SYSTEM AND INFORMATION INTEGRITY

SI.L1-3.14.2

Malicious Code Protection

DEGREE OF DIFFICULTY: EASY MEDIUM [✓ HARD]

Provide protection from malicious code at appropriate locations within organizational information systems.

WHAT: Figure out where protection from malicious code is needed and make sure you are providing protection at those locations.

HOW: Monitor for viruses or other malware at data entry and exit points, or at locations where there is a device like a firewall. Tools to do this range from off-the-shelf antivirus software to secure coding practices, which are common for OT.

MxD'S ADVICE / LESSONS LEARNED

- Keep antivirus software and virus scanners current.
- Use automatic software updates as one way to ensure patches and other fixes are installed as soon as they are available.
- Rely on application allowlisting so that only applications, files, and processes that are trusted can operate.
- Train employees so they do not plug in any personal or unscanned USB devices.
- Stay in touch with your equipment vendors to discuss their security practices, such as remote scanning, patch distribution, or other timely security communications.

IN DETAIL

MxD works with a lot of Department of Defense stakeholders so we know that USB drives are not authorized in many government environments. They can easily introduce malware into a system. Even though we knew stronger controls would not be needed until CMMC 2.0 Level 2, we decided to use software configurations to allowlist specific USB drives. That enables only MxD engineers to transport data to the factory floor via USB drives without risking the introduction of malicious code.

©2022 MxD, The Digital Manufacturing Institute | www.mxdusa.org

DOMAIN: SYSTEM AND INFORMATION INTEGRITY

SI.L1-3.14.4

Update Malicious Code Protection

DEGREE OF DIFFICULTY: EASY [✓ MEDIUM] HARD

Update malicious code protection mechanisms when new releases are available.

WHAT: Make sure the latest updates to all malicious code protections are installed as soon as possible. Other types of security patches may be scheduled for a later time if the security flaw has a lower severity or threat level.

HOW: Update company software and software tools, including antivirus programs, regularly.

MxD'S ADVICE / LESSONS LEARNED

- Remember, cybercriminals create new malware constantly. That means updates to block malicious code are absolutely crucial.
- Set a schedule for patching equipment. Updates can be automatic or manual; there are pros and cons to each update method. The important thing is to plan to do it.
- Balance the need for correcting security vulnerabilities against the time and effort required to update the equipment.

DOMAIN: SYSTEM AND INFORMATION INTEGRITY

SI.L1-3.14.5

System and File Scanning

DEGREE OF DIFFICULTY: EASY MEDIUM [✓ HARD]

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

WHAT: Scan systems and files for malicious code from external sources. Real-time scans can check new files as they are downloaded, opened, or saved. Scans also can check previously saved files for new malware.

HOW: Be aware that malicious code can find its way into your network in many ways: web pages, email, email attachments, portable storage devices, etc. Have your email provider set up a procedure to scan all attachments. Program antivirus software to scan computers daily. Don’t rely on employees alone to manage updates.

MxD’S ADVICE / LESSONS LEARNED

- Scan network information — such as files, databases, or other information systems — often enough to determine if unauthorized changes have been made.
- Make sure that whether you opt for automatic or manual scanning, this work is done only by an authorized person. Typically this is someone with administrative permissions for your network, for example, an IT or security employee.
- Use of USB drives is a common way to transfer information onto the factory floor. Be certain they’ve been scanned before they are plugged into machines.
- Scan the network configuration to ensure no unauthorized changes or additions have been made. Changes or additions may be signs of tampering.

Resources

MxD Cyber Marketplace

The MxD Cyber Marketplace provides cybersecurity assessments in an easy to understand format to help determine an organization's cybersecurity posture. Assessment outcomes are used to generate prioritized recommendations on the tools, services, and policies an organization should implement to close security gaps. Users can get quotes from leading tools and services providers from within the Marketplace, offering them a complete journey to strengthening their cyber defenses, from assessment to solution to implementation in an accessible environment. Learn more at **mxdusa.org/marketplace**.

MxD Virtual Training Center

MxD Learn, the workforce arm of MxD, has created the Virtual Training Center (VTC), a comprehensive training and learning platform designed to serve manufacturers and individual workers alike. The goal is to provide manufacturers with a first-of-its-kind platform to recruit and develop their workforce, encourage the use of cutting-edge technologies, and secure the workforce resiliency of their individual organizations and supply chains. Learn more at **mxdusa.org/vtc**.

Follow MxD on social media to stay updated on the latest announcements and resources.

linkedin.com/
company/MxD

@MxDInnovates

facebook.com/
MxDInnovates

@MxDInnovates

*Information for this Playbook came from the **CMMC Self-Assessment Guide Level 1** **https://www.acq.osd.mil/cmmc/docs/AG_Level1_V2.0_FinalDraft_20211210_508.pdf** and was used under the Creative Commons Attribution 4.0 International License. **https://creativecommons.org/licenses/by/4.0/***