CMMC COMPLIANCE WORKBOOK SERIES

WORKBOOK 2

Level 1 Compliance Workbook

FAR 52.204-21 Implementation Guide
for Small Defense Contractors

Applies To:	All DoD contractors handling Federal Contract Information (FCI)
Controls Covered:	15 controls — FAR clause 52.204-21(b)(1)
POA&Ms; Allowed:	NO — All 15 controls must be fully met before submission
Certification:	Annual self-assessment + affirmation submitted to SPRS
Phase 1 Status:	ACTIVE — Required in new DoD solicitations as of Nov 10, 2025
Version:	1.0 • March 2026

■ LEGAL DISCLAIMER — READ BEFORE PROCEEDING

This workbook is an educational and self-assessment tool. It does not constitute legal advice, cybersecurity consulting, or a guarantee of CMMC compliance. False certifications submitted to DoD may expose organizations and senior officials to False Claims Act (FCA) liability, including damages up to three times the value of the affected contract. Consult qualified legal counsel before submitting any compliance certification to the DoD.

HOW TO USE THIS WORKBOOK

Purpose

This workbook guides you through implementing all 15 cybersecurity controls required for CMMC Level 1. Each control gets its own page with the official verbatim requirement, plain-English translation, specific action steps, implementation tools, evidence checklist, and an interactive self-assessment status field. Use the companion Excel tracker (WB2_CMMC_Level1_Tracker.xlsx) alongside this guide to document your progress, asset inventory, and evidence.

Step 1	Read Section 1 to understand your scope — which systems and assets are covered.
Step 2	Open the companion Excel tracker (WB2_CMMC_Level1_Tracker.xlsx) and complete the asset inventory tab.
Step 3	Work through each of the 15 control pages. For each one: read, implement, then mark your status using the radio buttons.
Step 4	If a control is Not Met or Partially Met, note what is needed and track remediation in the Excel tracker. Remember: all 15 must be fully met before submitting — no Plan of Action & Milestones (POA&M;) is permitted at Level 1.
Step 5	Once all 15 controls are marked Met, use Section 3 to submit your self-assessment to SPRS.
Step 6	Have a senior official complete the annual affirmation in SPRS. Repeat every 12 months.

■ No POA&Ms; Permitted at Level 1

A Plan of Action & Milestones (POA&M;) is a documented list of gaps and remediation timelines. Unlike Level 2, CMMC Level 1 does NOT allow a POA&M.; All 15 controls must be FULLY implemented before you submit your self-assessment in SPRS. Submitting when controls are not fully met is a false certification and may expose your organization to False Claims Act liability.

SECTION 1 | Understanding Your Level 1 Scope

1.1 What Is In Scope?

Your Level 1 assessment covers all systems, devices, and locations that process, store, or transmit Federal Contract Information (FCI). This is called your **assessment scope**. Per the CMMC Level 1 Scoping Guide (dodcio.defense.gov), the following are considered **FCI Assets** and must be included:

Asset Type	What to Include
Computers & Laptops	Any device used to access, store, create, or transmit FCI — including personally owned devices if used for government contract work.
Servers & Network Storage	File servers, NAS devices, or cloud storage where FCI documents are stored.
Email Systems	Email accounts used to send or receive FCI — including Microsoft 365, Google Workspace, or on-premise mail servers.
Network Equipment	Routers, switches, and firewalls that carry FCI traffic on your network.
Mobile Devices	Smartphones and tablets used to access FCI email or documents.
Removable Media	USB drives, external hard drives, and other portable media used to store or transfer FCI.
Cloud Services	Any cloud platform (e.g., SharePoint, OneDrive, Dropbox) where FCI is stored or shared.

1.2 What Is Out of Scope?

The following are generally out of scope per the CMMC Level 1 Scoping Guide, provided they do not process, store, or transmit FCI:

- Personal devices used solely for non-work activities.
- Office equipment not connected to your network (standalone printers, fax machines).
- Systems used exclusively for publicly available information (public website servers).
- Contractor-operated systems fully isolated from FCI.

■ Document Your Scope in the Excel Tracker

Before beginning your self-assessment, create a written inventory of all in-scope assets in the WB2_CMMC_Level1_Tracker.xlsx asset inventory tab. This inventory is a key piece of evidence during any assessment review and is required for a complete self-assessment record.

SECTION 2 | The 15 FAR 52.204-21 Controls

The following pages cover each of the 15 controls required for CMMC Level 1. All control text is sourced verbatim from FAR clause 52.204-21(b)(1). Work through one control at a time — read, implement, document evidence in the Excel tracker, then mark your status using the interactive radio buttons.

Control ID	Domain	Control Name	Status
AC.L1-3.1.1	Access Control	Authorized Access Control	Met Partial Not Met
AC.L1-3.1.2	Access Control	Transaction & Function Control	Met Partial Not Met
IA.L1-3.5.1	Identification & Authentication	User Identification	Met Partial Not Met
IA.L1-3.5.2	Identification & Authentication	User Authentication	Met Partial Not Met
MP.L1-3.8.3	Media Protection	Media Sanitization	Met Partial Not Met
PE.L1-3.10.1	Physical Protection	Limit Physical Access	Met Partial Not Met
PE.L1-3.10.3	Physical Protection	Visitor Control	Met Partial Not Met
PE.L1-3.10.4	Physical Protection	Physical Access Logs	Met Partial Not Met
PE.L1-3.10.5	Physical Protection	Manage Physical Access Devices	Met Partial Not Met
SC.L1-3.13.1	System & Communications Protection	Boundary Protection	Met Partial Not Met

SC.L1-3.13.5	System & Communications Protection	Public-Access System Separation	Met Partial Not Met
SI.L1-3.14.1	System & Information Integrity	Flaw Remediation	Met Partial Not Met
SI.L1-3.14.2	System & Information Integrity	Malicious Code Protection	Met Partial Not Met
SI.L1-3.14.4	System & Information Integrity	Update Malicious Code Protection	Met Partial Not Met
SI.L1-3.14.5	System & Information Integrity	System & File Scanning	Met Partial Not Met

Source: FAR 52.204-21(b)(1). All 15 controls must be fully met before submitting your Level 1 self-assessment in SPRS. No partial credit or POA&M; is permitted at Level 1.

AC.L1-3.1.1

Access Control
Authorized Access Control

FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Only people, programs, and devices that are supposed to have access to your systems should be able to get in. This means having individual user accounts for each person, removing access when someone leaves, and not allowing unknown devices to connect.

WHAT YOU NEED TO DO

1. Create individual user accounts for every employee — no shared logins.
2. Maintain a written list of who is authorized to access each system.
3. Disable or delete accounts immediately when an employee leaves or changes roles.
4. Ensure all computers and devices on your network are inventoried and approved.
5. Review user access at least annually to confirm everyone listed still needs it.
6. Record your asset inventory and access list in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Windows Active Directory or local user accounts. Microsoft 365 user management. Windows Settings → Accounts for small shops. Document your user list in the companion Excel tracker.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ User account list showing all active accounts and their authorization.
- ■ Evidence of terminated accounts being disabled (screenshots, access logs).
- ■ System configuration showing login requirements are enforced.
- ■ Written policy or procedure for granting and revoking access.

■ Assessor Notes

This is the most fundamental access control. Every user must have their own account. Sharing passwords is a direct violation of this control.

Your Notes:

AC.L1-3.1.2 Access Control
Transaction & Function Control

FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Even authorized users should only be able to do what their job requires — this is called "least privilege." An office manager does not need access to engineering files; a field technician does not need payroll records.

WHAT YOU NEED TO DO

1. Review what each user role actually needs and limit access accordingly.
2. Restrict administrator privileges — only designated IT personnel should have admin rights.
3. Use folder and file permissions so employees can only access what they need.
4. Prevent standard users from installing software or changing system settings.
5. Document role-based access assignments in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Windows file and folder permissions (right-click → Properties → Security). Microsoft 365 role assignments. Avoid giving everyone admin rights on shared computers.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Role-based access matrix showing which users can access which systems/folders.
- ■ Evidence that admin privileges are restricted to designated personnel.
- ■ System or folder permission screenshots.
- ■ Written policy on least-privilege access.

Assessor Notes

Closely related to AC.L1-3.1.1. The distinction: 3.1.1 controls WHO can log in; 3.1.2 controls WHAT they can do once logged in. Both must be met.

Your Notes:

IA.L1-3.5.1 Identification & Authentication
User Identification

FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: ■ *enter here*

Assessor: ■ *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Every person, automated process, and device that accesses your systems must have a unique identity. No anonymous access, no shared "guest" accounts used for real work.

WHAT YOU NEED TO DO

1. Assign a unique username to every person who accesses any company system.
2. Remove or disable generic accounts (e.g., "admin", "user", "guest").
3. Ensure automated processes or service accounts have their own named identities.
4. Document all system identities in the asset and user inventory in your WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Windows local accounts or Active Directory. Microsoft 365 named user licenses. Disable the built-in "Guest" account on all computers (Windows Settings → Accounts).

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Full list of user accounts showing each has a unique identifier.
- ■ Evidence that guest/anonymous accounts are disabled.
- ■ Asset inventory showing devices are identified.

■ Assessor Notes

Identification (who are you?) is distinct from Authentication (prove it). This control covers identification only — IA.L1-3.5.2 covers authentication.

Your Notes:

IA.L1-3.5.2

Identification & Authentication
User Authentication

FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

After identifying who someone is, you must verify it — typically with a password. Everyone must log in with a password before accessing any system that handles Federal Contract Information (FCI). No passwordless access.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Require passwords on all computers, laptops, and mobile devices used for work. 2. Set password complexity requirements: minimum 8 characters, mix of character types. 3. Enable automatic screen lock after 15 minutes of inactivity. 4. Require passwords on all shared drives, cloud services, and email accounts. 5. Never allow blank or default passwords to remain on any system. 6. Document password policy in your WB2 Excel tracker.	Windows: Settings → Accounts → Sign-in options. Microsoft 365: password policies in Admin Center. Multi-factor authentication (MFA) is required at Level 2 but strongly recommended now.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Password policy documentation showing complexity and expiration requirements.
- ■ Screenshots of system sign-in requirements being enforced.
- ■ Screen lock timeout settings on all devices.
- ■ Evidence that default/blank passwords have been changed.

■ Assessor Notes

Passwords alone satisfy Level 1. However, enabling MFA now is best practice and prepares you for Level 2.

Your Notes:

MP.L1-3.8.3 Media Protection
Media Sanitization

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Sanitize or destroy information system media before disposal or reuse."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Before you throw away, sell, donate, or repurpose any computer, hard drive, USB drive, or other storage device that was used to store FCI, you must wipe it clean or destroy it. Simply deleting files is not enough — deleted files can be recovered.

WHAT YOU NEED TO DO

1. Before disposing of any hard drive or device: use an approved wiping tool or physically destroy it.
2. Track all media disposals — record what was wiped/destroyed, when, and by whom.
3. For drives that cannot be wiped (e.g., failed drives): physically destroy them.
4. Create a media sanitization policy that all employees must follow.
5. Apply this to all storage media: computers, laptops, USB drives, external drives, phones.
6. Log all disposals in the WB2 Excel tracker media sanitization log.

COMMON SMALL BUSINESS SOLUTIONS

Free tools: DBAN (Darik's Boot and Nuke) for hard drives. Eraser for Windows. For SSDs: manufacturer secure erase tools. For physical destruction: certified shredder or degausser.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Media sanitization log recording each disposal event.
- ■ Written sanitization policy or procedure.
- ■ Evidence of wiping tool used (e.g., DBAN completion screenshot).
- ■ Certificate of destruction if using a third-party shredding service.

■ Assessor Notes

This control is often overlooked. A common compliance failure is disposing of old computers without wiping them. Even a recycled computer with FCI on the drive is a violation.

Your Notes:

PE.L1-3.10.1 Physical Protection
Limit Physical Access

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Limit physical access to organizational information systems to authorized individuals."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: enter here

Assessor: enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Not everyone should be able to walk up to your computers and servers. Control who can physically access the machines that handle FCI — this means locked doors, access badges, or at minimum a secured area.

WHAT YOU NEED TO DO

1. Identify all physical locations where computers/servers handling FCI are located.
2. Restrict access to those areas to authorized personnel only.
3. Use locks, keycard access, or similar controls on server rooms or main office areas.
4. Ensure laptops and portable devices are secured when not in use.
5. Maintain a list of who has physical access to each location — document in WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Physical key locks, door access codes, keycard systems. For small businesses: a locked office or server closet is acceptable. Cable locks for laptops.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Description of physical access controls at each facility.
- ■ List of personnel with authorized physical access.
- ■ Photos or documentation of locks, badges, or access control systems.
- ■ Policy for securing portable devices.

Assessor Notes

For small businesses operating out of a single office, a locked door with limited key distribution often satisfies this control. Document what you have.

Your Notes:

PE.L1-3.10.3 Physical Protection
Visitor Control

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Escort visitors and monitor visitor activity."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

When visitors come to areas where FCI systems are located, they must be escorted by an authorized employee and their activity monitored. Visitors should never be left alone near your systems.

WHAT YOU NEED TO DO

1. Establish a visitor sign-in process (log with name, date, time in/out, and host).
2. Require employees to escort all visitors in areas where FCI systems are present.
3. Brief employees on the escorting requirement.
4. Post visitor policy at entry points if applicable.
5. Log all visitor activity in the WB2 Excel tracker visitor log.

COMMON SMALL BUSINESS SOLUTIONS

Simple visitor log (paper or spreadsheet). Badge visitors with "VISITOR" stickers. For smaller offices: a written procedure and consistent enforcement is sufficient.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- Visitor log showing sign-in/sign-out records.
- Written visitor policy or escorting procedure.
- Evidence of employee awareness (briefing records or posted policy).

Assessor Notes

Even in small offices, this control applies if visitors can see or access FCI systems. A simple sign-in sheet and escort policy satisfies the requirement.

Your Notes:

PE.L1-3.10.4 Physical Protection
Physical Access Logs

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Maintain audit logs of physical access."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Keep records of who accessed your facilities — both employees and visitors. These logs allow you to review who was where if an incident occurs and demonstrate that access is monitored.

WHAT YOU NEED TO DO

1. Maintain a physical access log for all entry points to areas with FCI systems.
2. Record: name, date, time in, time out, and purpose of visit.
3. Retain logs for a minimum of 90 days (longer is better).
4. Review logs periodically for unusual access patterns.
5. Store and maintain access logs in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Paper sign-in/sign-out sheets stored in a binder. Digital spreadsheet. Keycard access systems often generate automatic logs — export and retain these.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- Physical access log records (recent entries).
- Log retention policy stating how long logs are kept.
- Evidence that logs are reviewed (e.g., manager initials on log pages).

Assessor Notes

The visitor log from PE.L1-3.10.3 can double as the access log for this control if it captures all required information including employee entries.

Your Notes:

PE.L1-3.10.5 Physical Protection

Manage Physical Access Devices

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Control and manage physical access devices."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Keep track of and control all physical items that grant access to your facilities — keys, keycards, access codes, and badges. Know who has them, change them when needed, and account for them if lost.

WHAT YOU NEED TO DO

1. Maintain an inventory of all keys, keycards, and access codes.
2. Record who has been issued each key or credential.
3. Establish a process for reporting lost or stolen keys/cards.
4. Change access codes or rekey when an employee with access departs.
5. Conduct periodic inventory of all physical access devices.
6. Document key issuance and returns in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Key log spreadsheet. Physical key cabinet with checkout log. Rekey or change codes when employees leave. Document all issued credentials.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- Key/credential issuance log showing who holds each access device.
- Policy for managing lost/stolen access devices.
- Evidence that access was revoked or credentials changed upon employee departure.
- Periodic inventory records.

Assessor Notes

If you use a simple office key, document who has a copy and ensure you collect it (or rekey) when employees leave. This is often overlooked in small businesses.

Your Notes:

SC.L1-3.13.1 System & Communications Protection
Boundary Protection

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Monitor, control, and protect communications at the external boundaries of the information system and at key internal boundaries within the system."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Your network needs a firewall or similar device that controls what traffic comes in and goes out. You must protect the point where your internal network connects to the internet, and control traffic between different parts of your network.

WHAT YOU NEED TO DO

1. Ensure a firewall is enabled on your internet router/modem.
2. Enable the built-in firewall on all computers (Windows Defender Firewall).
3. Do not allow unknown or unapproved devices to connect to your network.
4. Segment guest Wi-Fi from your business network if visitors use Wi-Fi.
5. Review firewall rules periodically — block all traffic that is not needed.
6. Document your network boundary configuration in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Most business routers include a built-in firewall — ensure it is enabled. Windows Defender Firewall (built-in, free). Business-grade routers: Cisco Meraki, Ubiquiti, SonicWall. Separate guest Wi-Fi for visitors.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Network diagram showing boundary protection devices.
- ■ Firewall configuration documentation (screenshot or export).
- ■ Evidence that guest Wi-Fi is separated from business network.
- ■ Policy for connecting new devices to the network.

■ Assessor Notes

For most small businesses, a properly configured business router with firewall enabled plus Windows Defender Firewall on all computers satisfies this control.

Your Notes:

SC.L1-3.13.5 System & Communications Protection

Public-Access System Separation

FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Implement subnetworks for publicly accessible system components that are separated from internal networks."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

If you have any system or service the public can access (like a public website or customer portal), it must be on a separate network segment from your internal systems that handle FCI. This prevents public-facing systems from being used as a path into your internal network.

WHAT YOU NEED TO DO

1. Identify any systems accessible from the public internet (websites, portals, email servers).
2. Ensure those systems are hosted separately from your internal FCI systems.
3. If using cloud hosting (e.g., a website on AWS or GoDaddy), it is already separated — document this.
4. Do not host a public website on the same server or network as internal FCI systems.
5. Document your network separation in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Most small businesses use separate cloud hosting for websites (GoDaddy, Wix, AWS) — this naturally satisfies separation. If you run internal servers accessible from the web, consult an IT professional.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Network diagram showing separation of public-facing and internal systems.
- ■ Documentation of where public-facing systems are hosted.
- ■ Evidence that internal FCI systems are not reachable from the public internet.

Assessor Notes

Many small businesses satisfy this by simply using a third-party cloud host for their website. Document that your public systems are separate from internal systems.

Your Notes:

SI.L1-3.14.1 System & Information Integrity
Flaw Remediation

FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Keep your software, operating systems, and applications up to date. When security vulnerabilities are discovered in software you use, apply patches and updates promptly. Running outdated software is one of the most common causes of security incidents.

WHAT YOU NEED TO DO

1. Enable automatic updates on all computers running Windows or macOS.
2. Enable automatic updates for all software (browsers, Office, antivirus, etc.).
3. Establish a patch schedule: critical patches within 30 days, others within 90 days.
4. Keep a record of when patches are applied.
5. Include mobile devices and network equipment in your patching process.
6. Log patch activity in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Windows Update (Settings → Windows Update → enable automatic updates). Microsoft 365 automatic updates. Enable automatic updates in browser settings. Check vendor sites for network equipment firmware updates quarterly.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Screenshot of automatic update settings enabled on all systems.
- ■ Patch log or record of update activity.
- ■ Written patch management policy with defined timelines.
- ■ Evidence that all systems are running current, vendor-supported software versions.

Assessor Notes

Running unsupported software (e.g., Windows 7, Windows XP) is a direct violation. All systems must run versions with active security updates available from the vendor.

Your Notes:

SI.L1-3.14.2 System & Information Integrity
Malicious Code Protection

FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed: *enter here*

Assessor: *enter here*

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Install and maintain antivirus and anti-malware software on all computers. This software must be active, running, and updated to detect current threats. "Malicious code" includes viruses, ransomware, spyware, and trojans.

WHAT YOU NEED TO DO	COMMON SMALL BUSINESS SOLUTIONS
1. Install antivirus/endpoint protection on all computers and laptops. 2. Ensure real-time protection is enabled — not just scheduled scans. 3. Configure automatic updates for malware signature databases. 4. Run full system scans at least weekly. 5. Include mobile devices in your malware protection strategy. 6. Document your antivirus deployment in the WB2 Excel tracker.	Windows Defender (built-in, free — fully acceptable for Level 1). Malwarebytes Business. Bitdefender. CrowdStrike Falcon Go. Ensure Windows Defender is not disabled.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT
■ Screenshot showing antivirus software installed and active on all systems.
■ Evidence that real-time protection is enabled.
■ Antivirus update settings showing automatic definition updates are on.
■ Recent scan log showing successful scan completion.

■ Assessor Notes

Windows Defender, enabled and updated, fully satisfies this control for most small businesses. The key requirement is that it must be running and its definitions must be current.

Your Notes:

SI.L1-3.14.4	System & Information Integrity Update Malicious Code Protection	FAR 52.204-21

Official Requirement (FAR 52.204-21):

"Update malicious code protection mechanisms when new releases are available."

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Your antivirus and anti-malware tools must be kept current. When new malware definition updates are released, your systems must receive and apply them. Outdated malware definitions leave you vulnerable to threats that have emerged since the last update.

WHAT YOU NEED TO DO

1. Enable automatic definition updates for all antivirus software.
2. Verify that definition updates are being received daily (most tools do this automatically).
3. Document when and how updates are applied.
4. Review antivirus dashboard periodically to confirm updates are current.
5. Set up alerts if a system falls behind on updates.
6. Log update compliance in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Windows Defender updates automatically with Windows Update — ensure this is enabled. For third-party tools: enable automatic definition updates in product settings. Business endpoint tools typically have a management console showing update status.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Antivirus update configuration showing automatic updates enabled.
- ■ Recent update log or dashboard screenshot showing definitions are current.
- ■ Written policy requiring timely malware definition updates.

■ Assessor Notes

Closely related to SI.L1-3.14.2. Together: 3.14.2 requires antivirus is installed; 3.14.4 requires it is kept current. Both must be met independently.

Your Notes:

SI.L1-3.14.5	System & Information Integrity System & File Scanning	FAR 52.204-21

Official Requirement (FAR 52.204-21):

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

SELF-ASSESSMENT STATUS

- Met
- Partially Met
- Not Met

Date Assessed:
enter here

Assessor:
enter here

POA&M Required?

PLAIN-ENGLISH TRANSLATION

Two types of scanning are required: (1) scheduled full-system scans on a regular basis, and (2) real-time scanning that checks every file as it is opened, downloaded, or run. Both must be active simultaneously.

WHAT YOU NEED TO DO

1. Configure antivirus to scan all files in real-time as they are opened or downloaded.
2. Schedule full system scans at least weekly on all computers.
3. Enable scanning of email attachments before they are opened.
4. Scan all USB drives and external media when connected.
5. Review scan logs to confirm scans are completing successfully.
6. Document scan configuration and log results in the WB2 Excel tracker.

COMMON SMALL BUSINESS SOLUTIONS

Windows Defender: Settings → Virus & threat protection → Manage settings → enable Real-time protection. Schedule scans via Windows Task Scheduler or Defender settings. Microsoft Defender for Office 365 scans email attachments automatically.

EVIDENCE REQUIRED FOR SELF-ASSESSMENT

- ■ Antivirus settings showing real-time protection is enabled.
- ■ Scheduled scan configuration showing frequency and scope.
- ■ Recent scan logs confirming scans are completing successfully.
- ■ Email scanning configuration if applicable.

■ Assessor Notes

Real-time scanning is the most critical component of this control. Scheduled scans alone are insufficient — files must be scanned as they arrive. Confirm real-time protection is enabled.

Your Notes:

SECTION 3 | Submitting Your Level 1 Self-Assessment to SPRS

Once all 15 controls are fully implemented and documented in your Excel tracker, submit your self-assessment score and affirmation to the Supplier Performance Risk System (SPRS) at **sprs.csd.disa.mil**. SPRS is the DoD's official system for recording contractor compliance assessments. Your score and affirmation must be on file before you can be awarded contracts requiring CMMC Level 1.

3.1 Before You Start — Prerequisites

Prerequisite	Details
Active CAGE Code	Your company must have an active Commercial and Government Entity (CAGE) code. Register or verify at sam.gov.
Active SAM.gov Registration	Your System for Award Management (SAM.gov) registration must be current and active.
SPRS Account	You need an account at sprs.csd.disa.mil. Access is via DS Logon or CAC. If you do not have a DS Logon, create one at www.dmdc.osd.mil/self_service before proceeding.
All 15 Controls Met	Every control in Section 2 must be marked "Met" and documented in your Excel tracker. Level 1 score = 110 (all controls fully implemented).
Senior Official Identified	A senior official (owner, CEO, or authorized representative) must be available to complete the SPRS affirmation.

3.2 Step-by-Step SPRS Submission

Follow these steps to submit your Level 1 self-assessment.

STEP 1	Access SPRS
Navigate to sprs.csd.disa.mil in your web browser. SPRS requires a government-issued identity credential. Most small businesses use DS Logon (available at www.dmdc.osd.mil/self_service). If you do not have a DS Logon, create one before proceeding — allow 1–2 business days for account activation.	
URL:	*sprs.csd.disa.mil*
Login Method:	*DS Logon or CAC/PIV*

STEP 2 — Navigate to Self-Assessment Entry

After logging in, locate the "Assessments" menu in the top navigation. Select "NIST SP 800-171 Assessment" from the dropdown. On the assessment type screen, select "Level 1 (FAR 52.204-21)" to begin a new Level 1 entry.

Menu Path:	*Assessments → NIST SP 800-171 Assessment*
Assessment Type:	*Level 1 (FAR 52.204-21)*

STEP 3 — Enter Your Organization Information

Enter your company's CAGE code and verify that your organization information is current. Confirm your legal business name, address, and primary contact match your SAM.gov registration exactly.

CAGE Code:	■ *your 5-character CAGE code*
Org Name:	■ *must match SAM.gov exactly*

STEP 4 — Enter Your Self-Assessment Score

For a fully compliant Level 1, your score is 110 — the maximum. Enter 110 as your score. Select today's date as the assessment date. Enter the name and title of the person who conducted the assessment. The scope description should identify which systems and locations were assessed — use your Excel tracker asset inventory as the basis.

Score:	*110 (all 15 controls fully met)*
Assessment Date:	■ *today's date*
Conducted By:	■ *assessor name and title*
Scope:	■ *brief description of systems assessed*

STEP 5 — Complete the Senior Official Affirmation

A senior official must electronically affirm the accuracy of the self-assessment in SPRS per 32 CFR Part 170. The affirming official must have authority to legally bind the organization — typically the owner, CEO, President, or authorized compliance officer. See Section 4 for the exact affirmation language.

Official Name:	■ *full legal name of affirming official*
Title:	■ *owner / CEO / authorized officer*
Date of Affirmation:	■ *date signed in SPRS*

STEP 6	Submit and Retain Confirmation
Review all entries for accuracy, then submit. SPRS will generate a confirmation number and record the submission date. **Save or print the confirmation page immediately.** Record the confirmation number in your Excel tracker. Retain this record for the duration of your contract plus three years.	
Confirmation Number:	■ *record and save immediately*
Submission Date:	■ *record in Excel tracker*

SECTION 4 | Annual Affirmation & Renewal Requirements

4.1 The Annual Requirement

Per 32 CFR Part 170, CMMC Level 1 certification is not a one-time event. Every 12 months your organization must complete all three of the following:

■ Re-conduct the self-assessment

Complete all 15 controls again to confirm they remain fully implemented and update your Excel tracker.

■ Re-submit your score to SPRS

Enter a new assessment record in SPRS reflecting the current assessment date and score of 110.

■ Senior official affirmation

A senior official must submit a new affirmation in SPRS within the same annual cycle.

■ Lapse = Loss of Eligibility

If your annual self-assessment or affirmation lapses, your CMMC Level 1 certification is no longer valid and you will be ineligible for new DoD contract awards requiring CMMC until you complete a new submission. Set a calendar reminder 30 days before your annual renewal date and track it in your Excel tracker.

4.2 Official Affirmation Language

The following is the affirmation statement per 32 CFR Part 170.

Official Affirmation Statement (32 CFR Part 170):

"As a senior official of [Company Name], I affirm, to the best of my knowledge and belief, that [Company Name] has implemented the security requirements in FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, as described in the NIST SP 800-171 DoD Assessment submitted to the Supplier Performance Risk System (SPRS)."

The affirming official acknowledges that a knowing submission of false information may subject the organization and its officers to civil or criminal liability under the False Claims Act (31 U.S.C. § 3729) and other applicable law.

4.3 Annual Renewal Tracking

Initial Assessment Date:	■ *enter date*
Initial SPRS Submission Date:	■ *enter date*
Initial Affirmation Date:	■ *enter date*
Year 1 Renewal Due Date:	■ *enter date*
Year 1 Assessment Completed:	■ *enter date*
Year 1 SPRS Submission Date:	■ *enter date*
Year 2 Renewal Due Date:	■ *enter date*
Year 2 Assessment Completed:	■ *enter date*

This workbook is an educational and self-assessment tool. It does not constitute legal advice or a guarantee of CMMC compliance. Retain all completed assessment records for the duration of your contract plus three years. Re-evaluate any time your systems or contracts change.