JPert INC
Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · GOVERNMENT CONTRACTORS

Government Contractor IT Setup Guide: CMMC and NIST 800-171

How small federal contractors and subcontractors should set up IT to protect Federal Contract Information and Controlled Unclassified Information. Each step says plainly what your contract clauses **require** today, what is **recommended**, and what is only **proposed**.

By Umair Akhtar, Founder & President, JPert INC
Published November 1, 2026
Last reviewed November 1, 2026
About a 14-minute read

JPert INC
1934 Old Gallows Road, Suite 360, Vienna, VA 22182
703-576-8200 · jpert.com
Free to share. The latest version is always at https://jpert.com/white-papers/government-contractor-it-setup

Scan for the latest version

The short version

- The government paused the certificate, not the controls. On July 13, 2026, the Department of Defense suspended CMMC Phase 2, so solicitations can only ask for CMMC Level 1 or Level 2 self-assessments for now.
- DFARS 252.204-7012, the 110 requirements of NIST SP 800-171 Revision 2, SPRS scores and annual affirmations all still apply. So does False Claims Act liability for inaccurate security claims.
- If you only handle Federal Contract Information, you need the 15 basic safeguards in FAR 52.204-21 (CMMC Level 1) and an annual self-assessment.
- Keeping Controlled Unclassified Information in a small, separate enclave for the few people who need it can shrink what has to meet the full 110 requirements.

Who this is for and how to read it

This white paper is for owners, facility security officers and IT leads at federal contractors and subcontractors with roughly 5 to 100 people, especially Department of Defense suppliers. Every recommendation is labeled:

- **REQUIRED** A regulation or contract clause requires it today.
- **RECOMMENDED** Official guidance recommends it.
- **PROPOSED** It is in a proposed rule and is not yet required.

Your obligations come from the clauses in your contracts. This is general guidance, not legal advice; confirm specifics with your contracting officer and counsel.

The rules that apply today

Federal Contract Information: FAR 52.204-21

REQUIRED Contractors whose systems hold Federal Contract Information (FCI), information provided by or generated for the government under a contract that is not intended for public release, must meet the 15 basic safeguarding requirements in FAR 52.204-21. Under CMMC these are Level 1, with an annual self-assessment and affirmation. Plans of action (POA&Ms) are not allowed at Level 1.

Controlled Unclassified Information: DFARS 252.204-7012

REQUIRED DoD contractors that handle Controlled Unclassified Information (CUI) must comply with DFARS 252.204-7012, which requires:

- Implementing NIST SP 800-171 on systems that handle CUI.
- Reporting cyber incidents to DoD within **72 hours** through the DIBNet portal, which requires a DoD-approved medium assurance certificate. Get the certificate before you need it.
- Preserving images of affected systems for **90 days**.
- Using cloud services that meet security requirements equivalent to the **FedRAMP Moderate** baseline when they store or process CUI.
- Flowing the clause down to subcontractors that handle CUI.

The CMMC program

REQUIRED The CMMC program rule (32 CFR Part 170) took effect December 16, 2024, and the DFARS rule that puts CMMC into contracts took effect November 10, 2025, which started Phase 1. Level 2 covers the 110 requirements of NIST SP 800-171 Revision 2, with a minimum score of 88 of 110 to use a plan of action, and open items closed within 180 days. Level 3 adds 24 requirements from NIST SP 800-172. At every level, a senior "Affirming Official" affirms compliance in the Supplier Performance Risk System (SPRS).

What changed in July 2026

On July 13, 2026, DoD suspended Phase 2 of the CMMC rollout, which had been due to begin November 10, 2026, and put later phases on hold. The implementing memo limits solicitations to "CMMC Level 1 (Self) or CMMC Level 2 (Self)" and tells program offices to remove third-party (C3PAO) and DIBCAC assessment requirements from active solicitations and, at the next option or modification, from existing contracts. It keeps DFARS 252.204-7012 and NIST SP 800-171 Revision 2 as the baseline. Voluntary third-party assessments remain available. DoD has said it is reviewing the program; check the DoD CIO CMMC page for the latest status before you rely on any date.

Why this does not mean "relax": the Department of Justice continues to settle False Claims Act cases over NIST 800-171 gaps. In 2026, Honeywell Aerospace agreed to pay $2,042,518 (September) and LOGZONE agreed to pay $507,144 (June). Prime contractors also keep their own supplier security requirements.

Proposed, not yet required

- PROPOSED NIST published Revision 3 of SP 800-171 in May 2024 and withdrew Revision 2, but DoD has kept Revision 2 as its requirement for now. A pending DoD rule would move CMMC to **Revision 3**; until it is final, build to Revision 2.
- PROPOSED A civilian-agency **FAR CUI rule** was re-proposed on June 23, 2026, with Revision 3, 72-hour incident reporting and FedRAMP Moderate-equivalent cloud requirements. It is not final.

Our advice: build to Revision 2 today, and keep a simple map of how your controls line up with Revision 3 so a future change is a paperwork exercise, not a rebuild.

Step 1: Find your CUI and draw the boundary

REQUIRED CMMC Level 2 applies to the systems that process, store or transmit CUI, plus the security tools that protect them. So the first job is knowing where CUI actually

lives: which contracts carry it, which people touch it, and which email, file shares, laptops and cloud services hold it.

- RECOMMENDED **Consider an enclave.** If only a few people work with CUI, keeping it in a separate, locked-down environment for those users can shrink what must meet all 110 requirements, while the rest of the company runs on a simpler setup.
- REQUIRED **Write it down.** NIST SP 800-171 requires a System Security Plan describing the boundary and how each requirement is met.
- REQUIRED **Cloud services that hold CUI** must meet FedRAMP Moderate or DoD's equivalency requirements (DoD CIO memo, December 21, 2023). Cloud productivity suites offer different tiers: commercial tiers are generally suited to FCI only, government community tiers to some CUI, and high-assurance government tiers to export-controlled data. Confirm with your provider and contracting officer which tier fits your contracts.

Step 2: Accounts, passwords and multi-factor sign-in

- RECOMMENDED **Multi-factor sign-in (MFA) on email, remote access, cloud apps and every admin account.** CISA's ransomware guide asks for phishing-resistant MFA on all services, starting with email and remote access. Prefer an authenticator app, passkey or security key over text messages.
- RECOMMENDED **Long passphrases and a password manager.** Current NIST guidance (SP 800-63B, Revision 4) says passwords used alone should be at least 15 characters, should be checked against lists of leaked passwords, and should not be forced to change on a schedule unless there is a sign they were stolen.
- RECOMMENDED **One login per person and separate admin accounts.** Day-to-day work happens on standard accounts. Only a few people hold administrator rights, on separate logins.
- RECOMMENDED **Access ends on the last day.** When someone leaves, turn off email, remote access, shared passwords and building access the same day.

REQUIRED NIST SP 800-171 requires MFA for privileged accounts and for network access to non-privileged accounts in the CUI environment, plus limits on unsuccessful logins and session locks.

Step 3: Computers, phones and updates

- RECOMMENDED **Encrypt every laptop and phone** that holds work data, so a lost device is a hardware problem, not a data breach. NIST's small-business guide calls for full-disk encryption on laptops and tablets.
- RECOMMENDED **Turn on automatic updates**, and patch internet-facing systems and anything on CISA's Known Exploited Vulnerabilities list first.
- RECOMMENDED **Replace unsupported systems.** Windows 10 support ended October 14, 2025. Machines that cannot upgrade yet need Microsoft's paid Extended Security Updates, which are only available for a limited time, and should be replaced.
- RECOMMENDED **Endpoint protection that someone actually watches**, on every computer. Alerts that nobody reviews do not stop an attack.

REQUIRED In the CUI environment, NIST SP 800-171 requires protecting CUI on portable devices with encryption, controlling removable media, and fixing flaws in a timely way.

Step 4: Network, Wi-Fi and remote access

- RECOMMENDED **Separate networks** for staff computers, guest Wi-Fi, and printers, cameras and other smart devices. CISA calls for network segmentation and a current diagram of how data moves.
- RECOMMENDED **WPA3 Wi-Fi** where your equipment supports it, with a long passphrase that changes when staff leave. Guests get internet access only.
- RECOMMENDED **No remote desktop open to the internet.** CISA says remote desktop should never be exposed directly. Use a VPN or secure remote-access service with MFA.

- RECOMMENDED **A supported business firewall**, kept updated and replaced when the manufacturer stops supporting it.

REQUIRED NIST SP 800-171 also requires monitoring and controlling communications at the boundary of the CUI environment, protecting wireless access, and controlling remote access sessions.

Step 5: Logging, backups and your IT provider

- REQUIRED **Audit logs** in the CUI environment that let you trace actions to individual users, reviewed regularly. CISA recommends keeping critical system logs for at least a year.
- RECOMMENDED **Offline, encrypted, tested backups**, following CISA's ransomware guidance. DFARS 7012's 90-day image preservation rule makes good backups and logs doubly important.
- REQUIRED **Your IT provider is in scope.** Under the CMMC rule, a provider that manages your security tools is assessed as part of your environment even if it never touches CUI. Ask for its practices in writing.

RECOMMENDED In 2022, CISA, the NSA, the FBI and allied agencies published joint guidance for organizations that use a managed service provider (MSP). It says your contract should require MFA on every account the provider uses, least-privilege access, defined incident reporting, backup and incident-response duties, and prompt removal of the provider's access when the contract ends. Ask any IT provider, including us, to show you those terms in writing.

Step 6: Incidents and the 72-hour clock

- REQUIRED **Report to DoD within 72 hours** of discovering a cyber incident affecting covered defense information, through DIBNet. Have the required medium assurance certificate in hand before an incident.
- REQUIRED **Preserve images** of affected systems for 90 days.

- REQUIRED **Have an incident response capability** with preparation, detection, containment, recovery and testing, as NIST SP 800-171 requires. NIST SP 800-61, Revision 3 (April 2025) is the current federal reference.
- REQUIRED If personal information of Virginia residents is exposed, Virginia's breach law (Va. Code 18.2-186.6) may also require notice.

Step 7: Score honestly and affirm carefully

- REQUIRED **Post an accurate SPRS score** for each NIST 800-171 assessment, and keep it current.
- REQUIRED **Affirm only what is true.** The annual affirmation is signed by a senior official. Inaccurate affirmations are what False Claims Act cases are built on.
- RECOMMENDED **Track open items** in a plan of action with owners and dates, and close them.

One-page setup checklist

Area	What to have in place	Status today
FCI safeguards	15 FAR 52.204-21 requirements; annual Level 1 self-assessment and affirmation	REQUIRED
CUI boundary	Know where CUI lives; consider an enclave; System Security Plan	REQUIRED
NIST 800-171	110 Revision 2 requirements in the CUI environment; SPRS score posted	REQUIRED
Cloud	FedRAMP Moderate or equivalent for any cloud holding CUI	REQUIRED
MFA	Privileged and network access in the CUI environment; everywhere else too	REQUIRED CUI, RECOMMENDED elsewhere
Incident reporting	72-hour DIBNet report; medium assurance certificate ready; 90-day images	REQUIRED
Logs	User-traceable audit logs, reviewed; kept at least a year	REQUIRED logs, RECOMMENDED retention
Backups	Offline or locked copy; restores tested	RECOMMENDED
IT provider	Its security practices documented; in scope of your assessment	REQUIRED
Revision 3	Map controls to 800-171 Rev. 3 for when DoD moves	PROPOSED

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons. We help small contractors scope CUI, build enclaves, and keep the evidence that backs an SPRS score, and we document our own practices because a managed provider is part of your assessment. Read about IT for government contractors, or book a free IT assessment.

Related reading from our Chronicles: CMMC compliance checklist.

Sources

Every recommendation above comes from these official sources, checked on November 1, 2026:

- FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems
- DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting
- CMMC Program rule, 32 CFR Part 170 (Federal Register, October 15, 2024)
- DFARS CMMC acquisition rule (Federal Register, September 10, 2025)
- DoD CIO: Implementing the suspension of CMMC Phase II (July 2026)
- Cyber AB: Statement on the suspension of CMMC Phase II requirements
- NIST SP 800-171 Rev. 2: Protecting CUI in Nonfederal Systems (still required by DoD)
- DoD CIO: FedRAMP Moderate Equivalency memo (December 21, 2023)
- Federal Register: Re-proposed FAR CUI rule (June 23, 2026)
- DOJ: Honeywell Aerospace False Claims Act settlement (September 2026)
- DOJ: LOGZONE False Claims Act settlement (June 2026)
- CISA: #StopRansomware Guide
- CISA, NSA, FBI and allied agencies: Protecting against cyber threats to MSPs and their customers (AA22-131A)
- NIST SP 800-61 Rev. 3: Incident response recommendations (April 2025)

- NIST SP 800-63B Rev. 4: Authentication and passwords
- Va. Code 18.2-186.6 (breach of personal information notification)

This white paper is general information about IT and security practices, not legal advice. CMMC policy is changing; we review this paper when DoD announces changes. See our editorial policy.

FAQ

Common questions from contractors

Is CMMC third-party certification required in November 2026?

No. On July 13, 2026, the Department of Defense suspended Phase 2 of the CMMC rollout, which would have started requiring third-party assessments on November 10, 2026. For now, solicitations can only require CMMC Level 1 or Level 2 self-assessments. Check the DoD CIO CMMC page for updates.

Do we still have to meet NIST SP 800-171?

Yes. DFARS 252.204-7012 still requires NIST SP 800-171 for systems that handle Controlled Unclassified Information, along with 72-hour incident reporting. SPRS scores and annual affirmations still apply, and the Department of Justice continues to bring False Claims Act cases over inaccurate security claims.

Which revision of NIST SP 800-171 applies?

DoD currently requires Revision 2, with 110 requirements, even though NIST published Revision 3 in May 2024. A pending DoD rule would move CMMC to Revision 3, but it is not final. Build to Revision 2 and keep a map to Revision 3.

What does CMMC Level 1 require?

The 15 basic safeguarding requirements in FAR 52.204-21 for systems that hold Federal Contract Information, an annual self-assessment, and an annual affirmation in SPRS by a senior company official. Plans of action are not allowed at Level 1.

Want us to check your setup against this guide? Book a free IT assessment with our Vienna, VA team at jpert.com/contact or call 703-576-8200. We will give you a plain-English list of what to fix first.