

FIELD GUIDE

FAQ:

Demystifying
NIST SP 800-171 Rev. 3



SENTINELBLUE

SUMMARY

Who This Guide Is For

- Organizations Seeking Certification (OSCs)
- Federal contractors in the Defense Industrial Base
- Anyone with an interest in CMMC

What This Guide Contains

- FAQs about Rev. 3, including the transition from Rev. 2 and how it relates to the CMMC suspension

About Sentinel Blue Field Guides

Security is a team sport. We believe the Defense Industrial Base is stronger when knowledge and expertise are shared openly. That's why we've created free educational resources for federal contractors navigating cybersecurity and compliance challenges.

If you find this guide helpful, please share it with your community. Shields up!

FAQ: Demystifying NIST SP 800-171 Rev. 3

The timeline for transitioning from NIST SP 800-171 Rev. 2 to Rev. 3 has long been uncertain, and the CMMC Phase II pause has only added to it. The DoD currently maintains a class deviation that requires Rev. 2, but recent messaging signals an intent to eventually move to Rev. 3. One possible outcome of the ongoing CMMC review is that this transition finally begins.

So what does this mean for companies currently complying with Rev. 2? What will the transition actually look like, and how does the CMMC Phase II suspension factor in? We answer these questions and more below.

Q: Is Rev. 3 Just a Continuation of Rev. 2?

A: No, not really. Rev. 3 signals a shift from point-in-time readiness to continuous compliance, supported by strong security and effective documentation. It increases the maturity required from an organization with the addition of new control families, and it asks whether that organization can maintain operational resilience even as its systems, vendors, and threats change.



Q: What are ODPs, and why do they matter?

A: Organization-Defined Parameters. These are 88 new values, thresholds, and timeframes that Rev. 3 asks you to define yourself, unless the DoD has already set the definitions. For the ODPs that the DoD hasn't defined, your organization will need to document, justify, and consistently implement its choices.

Q: What are NFO controls, and why do they matter?

A: Non-Federal Organization controls, a.k.a. 61 basic security requirements. These controls were listed in the appendix of Rev. 2, but Rev. 3 has brought some of them explicitly into the standard.

Q: What changes does Rev. 3 include for controls?

A: There are three key changes to be aware of. First, controls have been consolidated from 110 down to 97, but more objectives have been added.

Second, three new control families have been introduced: Planning (PL), Systems and Services Acquisition (SA), and Supply Chain Risk Management (SR). These are governance and procurement functions, which means they lean heavily toward supply chain and vendor oversight as well as configuration management and incident response.

Third, there's closer alignment with NIST SP 800-53 Rev. 5, a.k.a. the federal government's broader security control catalog. A new CUI Overlay has been introduced to help organizations tailor the SP 800-53 moderate control baseline to protect CUI.

Q: What else should organizations know about Rev. 3 requirements?

- **3.4.8 requires application allow-listing**, i.e. a deny-all, allow-by-exception policy for software. Rev. 2 allowed either allow-listing or blocklisting, so if your organization is still running a blocklist model, this will be a major operational shift.
- **3.5.3 explicitly requires MFA for all system account access**, not just privileged and network access. (Check out our [detailed thoughts on MFA in the DIB.](#))
- **3.5.7 adds specificity around password protection** and reinforces the established NIST position on not requiring arbitrary password changes.
- **3.6.3 requires testing the *effectiveness* of a capability**, not just the capability itself. This makes explicit what was implicit in Rev. 2: strong security is the priority.
- **3.13.11 drops FIPS-validated modules** and instead requires organization-defined cryptography, one of the core recommendations in our [response to the CMMC Reform Task Force RFI](#).



Q: Is there any official date for Rev. 3 yet?

A: Not as of mid-September 2026. But the writing is on the wall: Rev. 3 will be required sooner rather than later, so it pays to start preparing now.

Q: How does this relate to the CMMC Phase II suspension?

A: The Phase II suspension applies only to the C3PAO assessment component of CMMC compliance. Defense contractors are still required to comply with the standards of NIST 800-171 Rev. 2, soon to be Rev. 3, as well as DFARS 252.204-7012. So, although the suspension means a temporary pause on external assessments, your underlying compliance obligations remain as strict as ever.

Q: What's the best plan of action while we wait?

A: We've laid out a more detailed guide in [this article](#), but here's the short version:

- Continue complying with NIST 800-171 Rev. 2. If you're already Level 2 certified, maintain your current CMMC practices.
- Read NIST's [Rev. 3 Small Business Primer](#), especially the tips for getting started with the three new control families.
- Review the DoD's [proposed Rev. 3 ODP values](#) and compare them against your own.
- Once you've understood the full requirements, you'll be ready to perform a detailed gap analysis and put together a plan of attack.



Is your organization ready for Rev. 3?

Let's talk.