SMB Challenges with NIST SP.800-171 Revision 3 Implementation

Authors:
Joy Beland and Scott Edwards, Summit 7 Systems
On behalf of the MSPs for the Protection of Critical Infrastructure
March 10, 2026

Abstract

Small and medium sized businesses (SMBs) in the federal supply chain face accelerating and sometimes conflicting requirements for safeguarding Controlled Unclassified Information (CUI). While the Department of Defense (DoD) continues to require NIST SP.800-171 Revision 2 (Rev. 2) and the General Services Administration (GSA) has moved to Revision 3 (Rev. 3), a governmentwide FAR CUI rule is poised to standardize expectations—but has not yet been finalized. This paper outlines five practical challenges SMBs encounter while implementing NIST SP.800-171 Rev. 3 (and, where relevant, Rev. 2) and offers considerations for aligning people, processes, and technologies amid cross-agency differences.

Author's Note on Scope

Although this paper focuses on NIST SP.800-171 Rev. 3, many SMBs are simultaneously subject to requirements referencing Rev. 2. Accordingly, certain challenges and recommendations herein address both revisions.

Introduction

For many SMB contractors, CUI obligations flow down from multiple federal agencies, each with distinct timelines, assessment frameworks, and incident reporting expectations. The result is a fragmented compliance landscape that complicates planning and strains limited resources. The following sections summarize the most consequential hurdles SMBs face as they operationalize NIST SP.800-171 controls across a sampling of contracts and agencies.

---

1. Cross-Agency Variability and Lack of Harmonization

The pending FAR CUI rule (anticipated clause FAR 52.204XX) is expected to establish a governmentwide baseline anchored to NIST SP.800-171 Rev. 2 and an 8-hour cyber-incident reporting timeline. Until that rule is finalized and implemented, however, agency specific directives remain in effect, creating divergent requirements for SMBs:

- Department of War (DoW) / DoD: Pursuant to Class Deviation 2024O0013 (issued May 2, 2024), contractors are directed to implement NIST SP.800-171 Rev. 2. Cyber incidents affecting Covered Defense Information must be reported within 72 hours under DFARS 252.204-7012.
- General Services Administration (GSA): As of January 5, 2026, GSA requires NIST SP.800-171 Rev. 3 as the baseline for contractor systems handling CUI and mandates a 1-hour reporting of CUI related cyber incidents under CIOIT Security 21112 Rev. 1.
- Department of Homeland Security (DHS): Per HSAR 3052.204-72 (Safeguarding of CUI), contractors are directed to implement a custom set of safeguarding controls and align with a 1- and 8-hour reporting requirement for cyber incidents involving CUI.
- Department of Energy (DoE) has issued DOE Order 471.7 and C2M2 requiring NIST SP 800-171 Rev 2 implementation with an 8-hour reporting requirement for incidents involving CUI.
- National Aeronautics and Space Administration (NASA) Requires implementation of NIST SP 800-171 Rev 2 under NASA Procedural Requirement (NPR) 2810.7, with a 1-hour reporting requirement for incidents involving CUI.
- Other Civilian Agencies: Upon finalization of the FAR CUI rule, these agencies are expected to align with the version specified in the final rule (currently Rev. 2) and adopt the eight-hour incident reporting window.

Implication for SMBs: Organizations working across agencies must reconcile multiple control baselines and uneven incident reporting timelines—from one hour (GSA) to eight hours (proposed FAR) to 72 hours (DFARS)—which complicates incident response planning, playbook design, and staffing.

---

2. Organizationally Defined Parameters (ODPs) in Rev. 3

NIST SP.800-171 Rev. 3 introduces additional Organizationally Defined Parameters (ODPs), requiring each organization to select values (e.g., session timeouts, password parameters, log retention) that meet agency expectations. While DoW has issued recommended values intended to reflect broad federal interests, non-DoW agencies may set different expectations.

Implication for SMBs: Without clear, agency specific ODP guidance, SMBs risk misalignment across contracts (e.g., password length/complexity, lockout thresholds, or data retention), leading to rework of configurations and documentation. Establishing a baseline with documented justifications and a deviation process is essential.

---

3. Divergent Third Party Assessment Requirements

Assessment pathways are not uniform:

- GSA requires use of a FedRAMP accredited 3PAO (or another assessor explicitly approved by GSA) for certification assessments involving CUI in contractor systems.
- DoW / CMMC Program requires assessment by a C3PAO (CMMC Third Party Assessment Organization) or a self-assessment depending on contract requirements.
- NASA, DoE, DHS and the Nuclear Regulatory Commission require self-attestation without a 3rd party validation.

Implication for SMBs: There is currently no reciprocity between these third party assessment credentials. SMBs supporting both environments may have to undergo separate assessment processes, increasing cost, scheduling friction, and audit fatigue.

---

4. External Service Provider (ESP) Criteria Gaps

External Service Providers (ESPs)—including Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs)—play critical roles in implementing and managing CUI relevant controls. Yet:

- The pending FAR CUI rule and GSA framework do not currently define uniform criteria for ESP eligibility or obligations.
- By contrast, the DoW's CMMC program specifies requirements for ESPs supporting CUI environments.

Implication for SMBs: Absent consistent federal criteria, SMBs must self-validate ESP capabilities and contractual commitments to ensure they are appropriate for CUI handling and aligned with the applicable control set (Rev. 2 or Rev. 3).

---

5. Sourcing Qualified MSPs/MSSPs and Solution Viability

SMBs frequently encounter challenges when evaluating MSPs/MSSPs:

- Incomparable Proposals: Pricing and scope vary widely, making "apples to apples" comparisons difficult.
- Qualification Uncertainty: Without a validated marketplace or universal credentialing for CUI service providers, SMBs may invest months (or longer) with consultants who cannot fully implement Rev. 2 or Rev. 3 requirements.
- Architectural Missteps: Misaligned solutions may suffice for generic security but fail to meet CUI handling constraints (e.g., enclave boundaries, data residency, logging depth, or multi-tenant separation), necessitating costly redesigns.

Implication for SMBs: Due diligence should extend beyond standard security claims to CUI specific architecture (e.g., boundary definition, identity isolation, device trust, and evidence generation) and to demonstrable audit readiness.

Recommendations

To mitigate the above challenges, SMBs can adopt the following practices:

1. Plan for the Stricter Requirement: Where agency demands conflict (e.g., GSA one hour vs. DFARS 72 hours), adopt the most stringent feasible standard enterprise wide to simplify playbooks and training.
2. Establish an ODP Governance Mechanism: Maintain a central ODP register with rationale, risk acceptance where applicable, and a contract specific deviation log to avoid ad hoc reconfiguration.
3. Design for Evidence: Build architectures that produce verifiable evidence mapped to NIST controls (e.g., immutable logs, alert artifacts, role based access reviews) to streamline any 3PAO/C3PAO assessment.
4. NIST can develop an augmented NIST SP 800-171 standard applicable to ESPs , with the current version 3 as the baseline. One certification for that updated standard can be accepted across federal agencies with reciprocity, so MSPs can offer standardized, affordable assistance to SMBs.
    a) In the meantime, SMBs can pre-qualify ESPs: Require prospective MSPs/MSSPs to provide proof of their own CMMC Level 2 Certification as well as a control-by-control shared responsibility matrices, sample system security plan (SSP) excerpts, runbooks, and evidence artifacts.
5. Harmonize Incident Response (IR) through CISA: CISA would act as a central clearing house for IR where businesses can report to a single agency and that agency is then responsible for reporting to all other federal agencies.
    a) Absent of a solution, SMBs can create a unified IR plan with configurable reporting timers (1hour / 8hour / 72hour) and agency specific notification trees, tested via cross agency tabletop exercises.
6. Maintain Dual Baselines During Transition: Until the FAR CUI rule is finalized and broadly implemented, preserve both a Rev. 2 and Rev. 3 baseline in your control library, with clear inheritance and compensating control narratives.
7. Contract Language Review: Where feasible, negotiate clarifying language on ODPs, assessment acceptance (e.g., potential reciprocity), and ESP responsibilities to reduce ambiguity before award.

Conclusion

SMBs operating in the federal supply chain are navigating a period of rapid change and partial misalignment in CUI safeguarding requirements. The emergence of NIST SP 800-171 Rev. 3, GSA's one hour reporting requirement, and the anticipated FAR CUI standard will ultimately drive greater uniformity—but, in the interim, SMBs must plan for cross agency variability. A governance model that harmonizes ODP selection, emphasizes evidence ready architecture through ESPs, and correlates reporting timelines will reduce rework, contain cost, and accelerate successful assessments—regardless of agency or revision.