securefort

FREE SELF-SCORING WORKSHEET

The SPRS Sanity-Check

Twenty minutes. Twenty-one questions.
Find out whether the score in SPRS is one your executive should be affirming.

Scoring basis: NIST SP 800-171 Revision 2 · DoD Assessment Methodology v1.2.1 · July 2026

What this worksheet does, and what it honestly cannot do

Somewhere in a government database called SPRS, your company probably has a score between negative 203 and positive 110. An executive at your company is required to personally affirm, every year, that the score is accurate and that compliance is continuous. In June 2026, the Department of Justice settled with a small defense contractor for $507,144 after a government assessment scored it at minus 170 against a high self-reported number. No whistleblower was involved. The government found it on its own.

This worksheet will not tell you your real score. A real score requires assessing all 110 requirements against evidence, and that takes two weeks, not twenty minutes. What twenty minutes *can* produce is something almost as useful: **your ceiling**. The twenty-one questions below cover the highest-value requirements in the official scoring methodology, the ones worth five points each, plus the two requirements with special graduated scoring and the one requirement that gates whether you have a score at all. Because the methodology only ever subtracts, honest answers here establish the highest number your real score could possibly be. The remaining 89 requirements can only pull it lower.

If your ceiling comes out below the number sitting in SPRS, you do not have a scoring problem. You have an affirmation problem, and it has a signature on it.

The rules, and they matter:

- Answer **Yes** only if you could produce evidence today: a screenshot, a configuration export, a record, a log, a document. If the honest answer is "I believe so," the answer is No. This is the standard a government assessor applies, so it is the standard this worksheet applies.
- If you do not know, the answer is No. Assessors do not score good intentions, and "I would have to check" from the person responsible is itself a finding.
- Do this with the person who actually administers your systems in the room, or on the phone. It goes faster and it stops the optimistic answers before they happen.

Question zero, before any points are counted

Q0. Do you have a System Security Plan that accurately describes your environment as it runs today: your real systems, your real boundaries, and how each of the 110 requirements is actually met?

A purchased template with the blanks filled in does not count. An SSP that names systems you do not own does not count; it counts against you.

If No: stop here. Under the official methodology, the absence of a System Security Plan means an assessment cannot be completed at all. The methodology's own words: the result is a finding that "an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012." Whatever number is in SPRS right now has no documented basis, and the affirmation attached to it is unsupported. That is worth knowing today rather than during an audit. The rest of the worksheet is still worth completing, because it shows you where remediation starts.

The twenty questions

Start at **110**. For every No, subtract the points shown. Questions 1 and 2 have a middle option; use it where it applies.

Identity and access

Q1. Is multifactor authentication enforced for every user, on every account: not just administrators, not just VPN users, everyone? *(Requirement 3.5.3)*

Yes: subtract 0 · Enforced for admins and remote access but not general users: subtract 3 · No or not enforced: subtract 5 ..... ____

Q2. Wherever encryption protects your CUI (laptops, VPN, file transfer), is it running in FIPS-validated mode, and could you name the validated module? *(Requirement 3.13.11)*

Yes: subtract 0 · Encryption yes, FIPS validation no or unknown: subtract 3 · No encryption in places CUI lives: subtract 5 ..... ____

Q3. Does every person have their own account, with no shared logins anywhere CUI is handled, including shop-floor and machine-transfer computers? *(Requirement 3.1.1)*

Yes: 0 · No: subtract 5 ..... ____

Q4. When someone leaves the company, is their access disabled the same day, and could you prove it for your three most recent departures? *(Requirement 3.9.2)*

Yes: 0 · No: subtract 5 ..... ____

Q5. Are phones and tablets that receive company email either enrolled in mobile device management or blocked from receiving CUI entirely? *(Requirement 3.1.18)*

Yes: 0 · No: subtract 5 ..... ____

Q6. Is your wireless network protected by per-user authentication (certificates or RADIUS), not a shared password? *(Requirement 3.1.17)*

Yes: 0 · No: subtract 5 ..... ____

Training

Q7. Has every employee completed security awareness training in the last year, and could you produce the completion records? *(Requirement 3.2.1)*

Yes: 0 · No: subtract 5 ..... ____

Q8. Have people with special responsibilities (IT, engineers handling CUI, shipping) received training specific to those duties? *(Requirement 3.2.2)*

Yes: 0 · No: subtract 5 ..... ____

Visibility

Q9. Are system logs from your servers and workstations collected centrally and retained on purpose, under a written retention period? *(Requirement 3.3.1)*

Yes: 0 · No: subtract 5 ..... ____

Q10. Does anyone actually review those logs on a schedule, with a record that the review happened? *(Requirement 3.3.5)*

Yes: 0 · No: subtract 5 ..... ____

Q11. Would anything alert you to an attack in progress: an off-hours login, a mass file transfer, a foreign connection? *(Requirement 3.14.6)*

Yes: 0 · No: subtract 5 ..... ____

Configuration and vulnerabilities

Q12. Do you have a documented baseline configuration for your systems and a maintained inventory, in writing, not in someone's head? *(Requirement 3.4.1)*

Yes: 0 · No: subtract 5 ..... ____

Q13. Has a vulnerability scan been run on your network in the last quarter, with results and a record of what was fixed? *(Requirement 3.11.2)*

Yes: 0 · No: subtract 5 ..... ____

Q14. Is every system that touches CUI on a patch cycle, including the ERP, the firewall, and the machines, not just Windows updates? *(Requirement 3.14.1)*

Yes: 0 · No: subtract 5 ..... ____

Incidents

Q15. Do you have a written incident response plan naming who decides, who calls whom, and what counts as an incident? *(Requirement 3.6.1)*

Yes: 0 · No: subtract 5 ..... ____

Q16. Could you file the 72-hour cyber incident report to DoD that DFARS 252.204-7012 requires, starting right now: do you have the DIBnet procedure and the DoD-approved medium assurance certificate it takes to submit one? *(Requirement 3.6.2)*

Yes: 0 · No: subtract 5 ..... ____

Media and passwords

Q17. Are USB drives and removable media controlled, so that only company-issued, encrypted devices work in your machines? *(Requirement 3.8.7)*

Yes: 0 · No: subtract 5 ..... ____

Q18. When drives, laptops, or machines leave your custody (disposal, repair, return), are they sanitized first, with a certificate or record kept? *(Requirement 3.8.3)*

Yes: 0 · No: subtract 5 ..... ____

Q19. Are all stored and transmitted passwords cryptographically protected, including inside line-of-business applications like your ERP? *(Requirement 3.5.10)*

Yes: 0 · No: subtract 5 ..... ____

Proof

Q20. Has anyone assessed your controls against all 110 requirements in the last year, with the results written down? *(Requirement 3.12.1)*

Yes: 0 · No: subtract 5 ..... ____

Your ceiling

Starting score	110
Total subtracted (Q1 through Q20)	____
Your ceiling	____
The score currently in SPRS	____

Your real score is at or below your ceiling. These twenty questions cover 100 of the 313 possible deduction points in the methodology; the other 89 requirements, the ones worth 3 points and 1 point, almost always find more. In our experience the honest full-assessment number lands 20 to 60 points below the worksheet ceiling for a typical small contractor.

Reading the result:

Ceiling 100 or above. Rare, and it means the fundamentals are in place. The open question is whether your evidence would survive an assessor, and whether the 89 remaining requirements hold up. A full assessment is confirmation, not rescue.

Ceiling between 60 and 99. You are approximately where the industry median sits. The gap is real but the path is short: most of what you subtracted above is discipline and configuration, not capital. The question that matters: is the number in SPRS above your ceiling? If so, keep reading.

Ceiling below 60, or negative. You are in the range where most honestly assessed small contractors actually land, so the number itself is not shameful. What it is, is unsignable. If an affirmation is coming up, this result is the reason to act on a schedule now rather than explain a schedule later.

Any ceiling below the number in SPRS. This is the result that matters regardless of band. The score on file is mathematically impossible if your answers above were honest. A company in Huntsville, Alabama learned in June 2026 what that costs when the government checks: $507,144, after government assessors scored it at minus 170 on the same scale where it had reported itself compliant. The fix is not complicated, but it does have an order: establish the real number against evidence, build the dated remediation record, then correct what is on file with counsel's guidance. Acting first is what separates an error from a false claim.

Three ways forward

Verify this yourself. Everything above traces to the NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, published June 24, 2020. It is public. Look up Annex A and check our point values; we would rather you trust the document than trust us.

See what a full assessment looks like. Our sample gap-assessment report shows the complete methodology applied end-to-end to a realistic 58-person machine shop, including the scoring table for all 110 requirements and the remediation math from a negative score back to 110. Request it at securefort.io.

Talk it through. Thirty minutes, no pitch, and if you do not need us we will say so on the call. The 2-week Defense Compliance Diagnostic ($7,500, credited in full toward the full Program within 90 days) replaces this worksheet's ceiling with a real, evidence-backed number and a prioritized plan. Book at securefort.io or write to hello@securefort.io.