TRUST CENTER | SECURITY & COMPLIANCE

NIST SP 800-171 Compliance:

What It Means, Why There Is No Formal Certification, and Why It Still Matters for Your Business

Understanding NIST SP 800-171

NIST Special Publication 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Black Box) establishes 110 security requirements across fourteen control families designed to safeguard Controlled Unclassified Information (CUI). Originally developed to protect sensitive federal data handled by contractors and suppliers outside government networks, its rigorous framework has become a widely recognized benchmark for cybersecurity maturity across both public and private sectors.

Why NIST SP 800-171 Does Not Result in a Formal Certification

Unlike frameworks such as ISO 27001 or FedRAMP, NIST SP 800-171 is a **self-attestation standard** — by design. NIST intentionally did not build a third-party certification program into SP 800-171 for several structural reasons:

- Scope Flexibility: Black Box has implemented the 110 controls in ways tailored to their unique environments, systems, and risk profiles. A single pass/fail certification cannot fairly accommodate this variability.
- Continuous Compliance Model: NIST 800-171 compliance is an ongoing operational posture, not a point-in-time audit event. The standard expects Black Box to continuously assess, document, and improve their security practices using a System Security Plan (SSP) and Plan of Action & Milestones (POA&M).
- Government Accountability: The standard is enforced contractually through the Defense Federal Acquisition Regulation Supplement (DFARS) and validated through self-attestation to the DoD's Supplier Performance Risk System (SPRS), placing accountability directly on Black Box rather than a certifying body.
- Note on CMMC: The Cybersecurity Maturity Model Certification (CMMC) framework incorporates NIST 800-171 at its core (CMMC Level 2).

The Business Value of NIST SP 800-171 Compliance

Compliance without certification is still a powerful trust signal. Here is what our NIST SP 800-171 posture means for organizations that partner with us:

✔ Federal & Defense Supply Chain Readiness

Our SPRS score and documented SSP demonstrate contractual eligibility to handle CUI, making us a low-risk partner for prime contractors, subcontractors, and any organization operating within the DoD supply chain.

✔ Reduced Third-Party Risk for Your Organization

When you partner with us, your vendor risk management obligations are simplified. Our documented security controls, policies, and continuous monitoring practices translate directly into reduced exposure in your own compliance and risk assessments.

✔ **Alignment With Leading Regulatory Frameworks**

NIST SP 800-171 controls map closely to NIST SP 800-53, HIPAA Security Rule safeguards, and ISO 27001 Annex A controls. Our compliance posture supports your broader regulatory obligations across industries and jurisdictions.

✔ **Demonstrated Security Maturity & Operational Discipline**

Maintaining 110 security requirements across access control, incident response, configuration management, and more reflects an organization-wide commitment to security — not a checkbox exercise. Our ongoing POA&M process ensures gaps are actively tracked and remediated.

What We Provide to Support Your Due Diligence

We make our compliance posture transparent and verifiable. Upon execution of an appropriate agreement, we can provide:

- A summary of our System Security Plan (SSP) addressing all fourteen control families
- Our current SPRS score and attestation documentation
- Our Plan of Action & Milestones (POA&M) status summary
- Completion of standard vendor security questionnaires (VSQs) and third-party risk assessments

---

Security Security & compliance inquiries:
For questions about our security posture or to request compliance documentation - Contact Us