GRYPHON
SECURITY

NIST SP 800-171 / CMMC Readiness Assessment

Clear Compliance Insight. Defensible Federal Readiness.

A focused readiness assessment designed for organizations that store, process, or transmit Controlled Unclassified Information (CUI) and must demonstrate compliance with federal cybersecurity requirements.

Federal contractors face a materially different risk profile than commercial organizations. Handling CUI introduces regulatory obligations under DFARS 252.204-7012 and increasing scrutiny through NIST SP 800-171 self-assessments, SPRS scoring, and CMMC Level 2 requirements. This service provides leadership with a clear, defensible understanding of current compliance readiness before an audit, score submission, or third-party assessment.

What We Do

We conduct a structured readiness assessment evaluating how your organization implements the 110 requirements of NIST SP 800-171 and how well those implementations can withstand federal or prime-contractor scrutiny.

The assessment reviews policies, procedures, technical controls, and evidence supporting your System Security Plan (SSP) and Plan of Action & Milestones (POA&M). Controls are evaluated as implemented, partially implemented, or not implemented, with findings mapped directly to SPRS scoring impact and CMMC Level 2 expectations.

The result is a practical, evidence-based view of readiness, not assumptions or aspirational documentation.

Why This Matters for Federal Contractors

Inadequate NIST SP 800-171 implementation exposes organizations to contract risk, adverse SPRS scores, flow-down violations, and failed CMMC assessments. More importantly, unsupported or inaccurate claims of compliance create defensibility risk under DFARS 7019 and 7020.

This assessment identifies where compliance gaps actually exist, distinguishes documentation gaps from technical failures, and provides leadership with a clear path to remediation before those gaps become contractual or legal issues.

Our Assessment Approach

This service uses a compliance-driven but practical methodology aligned to:

- NIST SP 800-171 Rev. 2
- DoD Assessment Methodology
- CMMC Level 2 assessment objectives

The assessment is **not a certification or C3PAO assessment**. It is a readiness engagement designed to answer one core question:

"Can this organization credibly demonstrate NIST SP 800-171 compliance if challenged?"

Findings are scoped to your actual CUI environment and supporting systems, ensuring recommendations are achievable and relevant.

What's Evaluated

The readiness assessment evaluates **all 14 NIST SP 800-171 control families**, including:

- Access Control
- Identification & Authentication
- Audit & Accountability
- Configuration Management
- Incident Response
- System & Communications Protection
- System & Information Integrity

Each control is reviewed for implementation status, evidence sufficiency, and SPRS scoring impact, with gaps clearly documented.

What You Receive

- Executive-level readiness summary
- Preliminary **SPRS score** based on observed evidence
- Control-by-control findings tied to NIST SP 800-171 requirements
- Clear identification of SSP and POA&M gaps
- A prioritized remediation roadmap aligned to CMMC readiness

Deliverables are structured to directly support SSP and POA&M development and future assessment preparation.

Who This Service Is For

This service is designed for:

- Defense contractors and subcontractors handling CUI
- Organizations preparing to submit or update an SPRS score
- Organizations planning for CMMC Level 2 Certification
- Leadership seeking defensible compliance clarity before audits

It is particularly valuable for organizations pursuing federal contracts that have not completed a required NIST SP 800-171 self-assessment and lack a clear approach to performing and documenting one.

Why Gryphon Security

- **Federal Compliance Focus**: Built specifically for NIST SP 800-171 and CMMC environments
- **Assessment-First Approach**: Evidence-driven, not assumption-based
- **Defensible Outcomes**: Findings leadership can stand behind
- **NIST-Based**: Grounded in federal assessment methodology
- **Independent & Vendor-Neutral**: No resale pressure, no tool bias

Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm CUI scope and system boundaries
- Discuss current SSP and SPRS status
- Explain exactly what the readiness assessment will and will not cover

We will not pressure you into tools, managed services, or long-term contracts.

Gryphon Security, LLC
Cybersecurity for Federally Regulated Environments
info@gryphonsec.com | www.gryphonsec.com