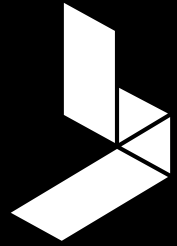


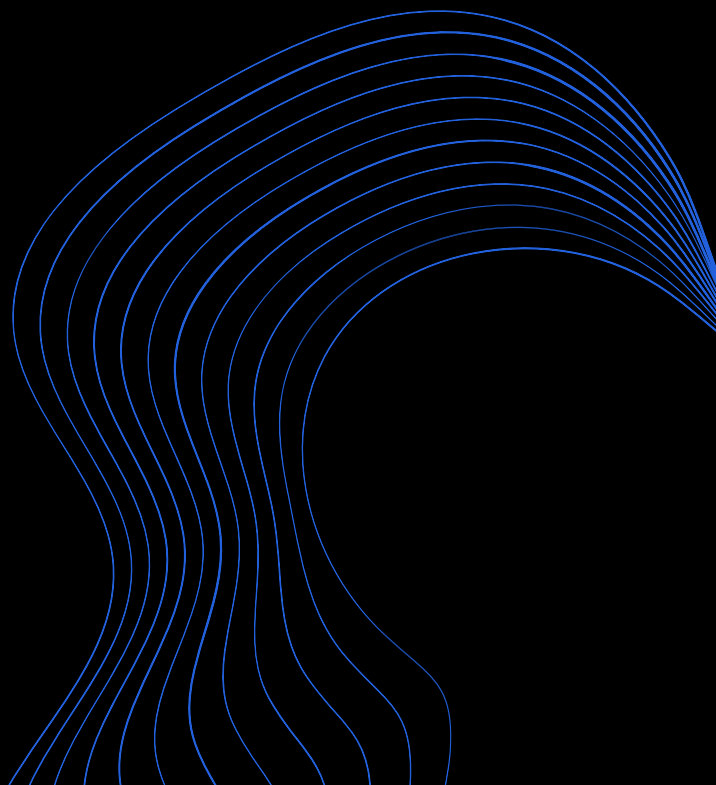


BitLyft




THE COMPLETE **NIST 800-171** GUIDE

**HOW TO MEET
CYBERSECURITY
COMPLIANCE AND
PROTECT UNCLASSIFIED
INFORMATION (CUI)**





INDEX

- 
- 1 Introduction**
 - 2 What is NIST 800-171**
 - 3 Who Needs to Comply**
 - 4 14 Control Families**
 - 5 Core Functions & Expectations**
 - 6 Compliance Roadmap**
 - 7 Assessment, scoring, and Monitoring**
 - 8 NIST vs. CMMC**
 - 9 Importance of NIST**
 - 10 How BitLyft Simplifies**
 - 11 Glossary**



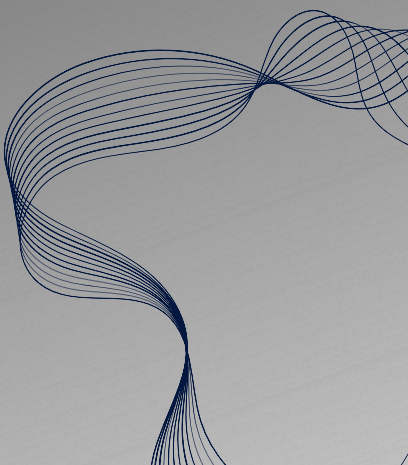
INTRODUCTION

Cybersecurity expectations for government contractors and their partners have evolved dramatically. Data once considered low-risk—like design files, project schedules, or vendor correspondence—is now recognized as controlled and valuable to adversaries.

With increasing cyberattacks and federal oversight, protecting sensitive information isn't optional—it's mandatory. The challenge? Many organizations aren't sure where to begin.

NIST SP 800-171 provides the blueprint for protecting Controlled Unclassified Information (CUI) on non-federal systems. While the framework may seem complex at first glance, understanding it empowers organizations to strengthen defenses, win government contracts, and build a foundation for long-term security maturity.

This guide breaks down what NIST 800-171 is, why it matters, how to comply, and how BitLyft helps simplify the process.





WHAT IS NIST 800-171?

The National Institute of Standards and Technology (NIST) developed Special Publication (SP) 800-171 to define how non-federal organizations should safeguard Controlled Unclassified Information (CUI). It establishes a consistent set of cybersecurity requirements across 14 control families, designed to protect data confidentiality, integrity, and availability.



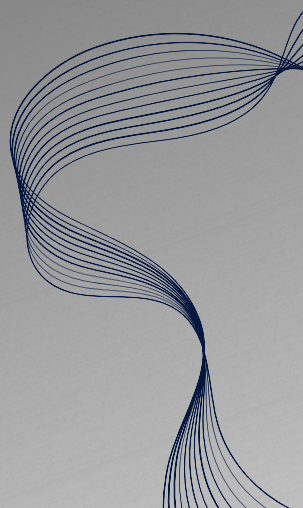
Purpose

To create a repeatable, scalable framework that helps organizations protect government-related information while maintaining operational flexibility.



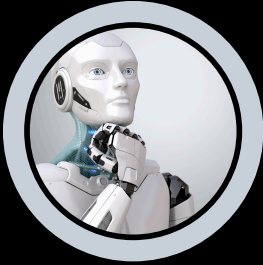
Relationship to Other Frameworks

NIST 800-171 draws from NIST SP 800-53, the broader federal cybersecurity standard, and serves as the foundation for the Cybersecurity Maturity Model Certification (CMMC).



WHO NEEDS TO COMPLY

Any organization that stores, processes, or transmits CUI under a federal contract must comply with NIST 800-171.



Prime contractors & subcontractors

working with the
Department of
War (DOW)



Vendors & service providers

handling CUI in IT,
manufacturing, or
logistics



Universities & research institutions

receiving federal
funding



Cloud service providers

hosting federal
or defense-
related data

→ *WHY IT MATTERS*

- 1. Legal Requirements** – Under DFARS 252.204-7012 and related clauses, compliance is mandatory.
- 2. Competitive Advantage** – Demonstrating NIST compliance enhances trust and contract eligibility.
- 3. Security Resilience** – Adherence helps prevent costly breaches and data leaks.
- 4. Future Readiness** – Compliance prepares you for CMMC 2.0 certification.

Noncompliance risks include contract loss, penalties, and potential False Claims Act violations for inaccurate self-assessment reporting.



14 Control Families

- 1. Access Control (AC)** – Limit access to authorized users and devices.
 - 2. Awareness & Training (AT)** – Ensure personnel understand cybersecurity responsibilities
 - 3. Audit & Accountability (AU)** – Track system activities to detect and analyze incidents.
 - 4. Configuration Management (CM)** – Establish secure baseline configurations and manage system changes.
 - 5. Identification & Authentication (IA)** – Verify user identities and enforce strong authentication.
 - 6. Incident Response (IR)** – Prepare for, detect, and respond to security incidents.
 - 7. Maintenance (MA)** – Manage and control system maintenance activities securely.
 - 8. Media Protection (MP)** –Safeguard data on physical and digital media.
 - 9. Personnel Security (PS)** – Screen and manage personnel before granting system access.
 - 10. Physical Protection (PE)** –Limit physical access to systems and facilities.
 - 11. Risk Assessment (RA)** – Identify and prioritize cybersecurity risks.
 - 12. Security Assessment (CA)** – Periodically evaluate and verify control effectiveness.
 - 13. System & Communications Protection (SC)** – Protect network boundaries and communications.
 - 14. System & Information Integrity (SI)** –Detect, report, and correct system flaws and malicious activity.
- 



Core Functions


1. **Identify** – understand what data, systems, and users exist.
2. **Protect** – Implement safeguards such as MFA, encryption, and access control.
3. **Detect** – Monitor systems for anomalies and unauthorized activity.
4. **Respond** – Contain, analyze, and remediate incidents.
5. **Recover** – Restore operations and learn from incidents.



WHAT TO EXPECT

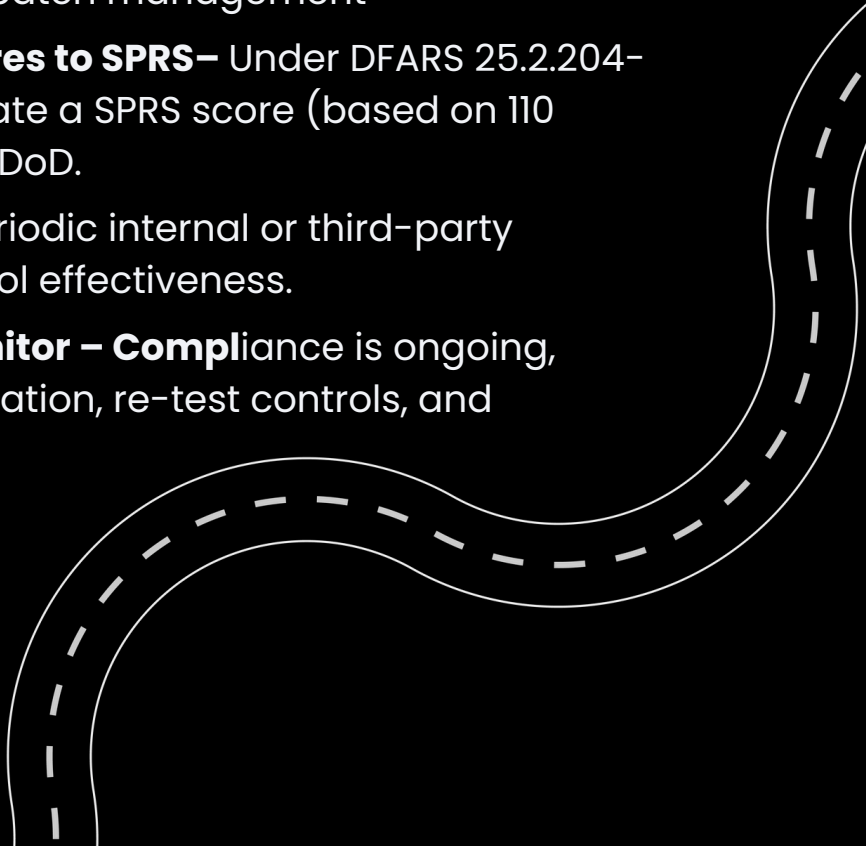
- ✓ **Documentation** – Building accurate SSP and POA&M records.
- ✓ **Implementation** – Applying controls and improving processes.
- ✓ **Validation** – Verifying security performance through audits or assessments.
- ✓ **Maintenance** – Continuous improvement through monitoring and updates.

Compliance may seem complex, but with the right partner, it becomes a structured, achievable journey.





The NIST 800-171 Compliance Roadmap

- 1. Define Scope & Identify CUI** – locate where CUI resides, how it moves, and who accesses it.
 - 2. Conduct a Gap Assessment** – compare existing controls to NIST 800-171 requirements using NIST SP 800-171A or a trusted partner.
 - 3. Develop a System Security Plan (SSP)** – Document your implemented and planned security controls. This is your living compliance record.
 - 4. Create a plan of Action & Milestones (POA&M)** – Outline deficiencies, target completion dates, and responsible parties.
 - 5. Implement Required Controls** – apply technical safeguards such as:
 - Multi-factor authentication (MFA)
 - Encryption (FIPS-validated)
 - Endpoint protection and SIEM integration
 - Secure configuration and patch management
 - 6. Report Self-Assessment Scores to SPRS** – Under DFARS 25.2.204-7019, contractors must calculate a SPRS score (based on 110 controls) and submit it to the DoD.
 - 7. Validate & Audit** – Perform periodic internal or third-party assessments to confirm control effectiveness.
 - 8. Maintain & Continuously Monitor** – **Compliance** is ongoing, continue to update documentation, re-test controls, and monitor threats continuously.
- 

Assessment, Scoring, and Continuous Monitoring

Each of the 110 NIST controls is assigned a value. Organizations start at 110 points and subtract points for unmet requirements.

Scores range: -203 to 110

Submission: Required in the DoD's Supplier Performance Risk System (SPRS).

Goal: Demonstrate progress toward full implementation with supporting documentation (SSP and POA&M).

Continuous Monitoring

Maintain compliance by:

- Automating log collection and alerting
- Conducting quarterly control reviews
- Revalidating access lists and configurations
- Training employees regularly

Proactive monitoring helps prevent drift and ensures compliance readiness for audits or CMMC certification.

NIST vs. CMMC

Aspect	NIST 800-171	CMMC 2.0
Purpose	Defines <i>what</i> security controls must exist	Defines <i>how</i> compliance is assessed
Orgin	Created by NIST	Managed by the DoD
Structure	110 requirements across 14 control families	3 maturity levels based on NIST controls
Assessment	Self-assessment (SPRS submission)	Third-party or DoD assessment
Focus	"Do this"	"Prove you've done it"

NIST = the standard. CMMC = the certification.

Organizations compliant with NIST 800-171 are already 80–90% of the way toward CMMC Level 2 readiness.



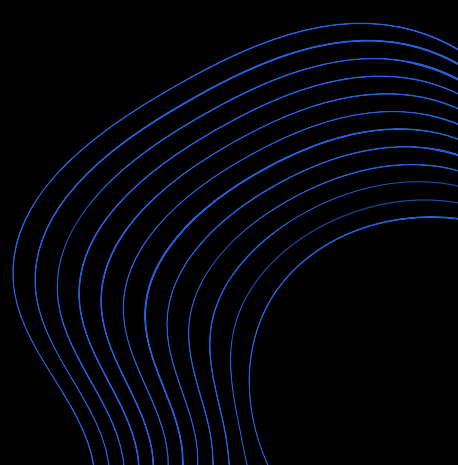
How BitLyft Simplifies Compliance

At BitLyft, we transform compliance from a burden into a strength. Our True MDR platform is powered by BitLyft AIR®. Bringing automation, intelligence, and human expertise to streamline security operations and compliance maintenance.

Core Capabilities

1. **Security Information & Event Management (SIEM)** – AU, SC, SI: centralized log management and anomaly detection.
2. **Security Orchestration, Automation & Response (SOAR)** – IR, SI: automated incident response and remediation
3. **User & Entity Behavior Analytics (UEBA)** – AC, AU, IA: detects insider threats and unauthorized access.
4. **Central Threat Intelligence (CTI)** – RA, CA, SC: contextual threat awareness and proactive defense
5. **SOC Expertise** – AT, IR, SI: real-time human analysis and escalation.

With BitLyft, you gain:

- ➔ 24/7 monitoring and automated detection
 - ➔ Integrated compliance reporting for NIST & CMMC
 - ➔ Tier 3 SOC analysts as an extension of your team
 - ➔ Simplified evidence collection for audits
- 



GLOSSARY



CUI: Controlled Unclassified Information

DFARS: Defense Federal Acquisition
Regulation Supplement

SSP: System Security Plan

POA&M: Plan of Action and Milestones

SPRS: Supplier Performance Risk System

CMMC: Cybersecurity Maturity Model
Certification

SIEM: Security Information and Event
Management

SOC: Security Operations Center

SOAR: Security Orchestration,
Automation, and Response