TRNSFRM
Cybersecurity. Compliance. Managed IT.

LEAD MAGNET · 2026 EDITION

The Manufacturer's Guide to NIST 800-171

Translating 110 technical controls into an actionable, audit-ready roadmap — built around the IT Resilience Framework™.

Prepared by TRNSFRM · Cleveland · Columbus · Nationwide

TRNSFRM
Cybersecurity. Compliance. Managed IT.

Audit-ready is
operations

If your shop floor touches Controlled Unclassified Information (CUI), DFARS 252.204-7012 and CMMC 2.0 obligate you to implement all 110 NIST 800-171 controls — and to prove it with a System Security Plan (SSP), a Plan of Action & Milestones (POA&M), and a verifiable SPRS score.

This guide cuts through the 14 control families and rewrites them as a manufacturer-friendly playbook: what to do, who owns it, what evidence to keep, and how to roll it up to a repeatable assessment.

110	14	3	110pt
SECURITY REQUIREMENTS	CONTROL FAMILIES	RESILIENCE PHASES	SPRS SCORE TARGET

Who this is for

- Manufacturers in the DoD / aerospace / defense supply chain handling CUI, ITAR, or covered defense information.
- Tier 2 and Tier 3 suppliers preparing for CMMC Level 2 third-party assessment (C3PAO).
- IT & operations leaders who need a non-jargon roadmap they can execute with a small team.

THE OPERATING MODEL

The IT Resilience Framework™

We sequence NIST 800-171 work across three phases. Each phase produces tangible artifacts an assessor (or your prime contractor) can verify.

01 ASSESS — Establish the truth.

Scope CUI, inventory assets, run a control-by-control gap assessment, baseline your SPRS score, and produce the first SSP draft.

Artifacts produced: CUI data-flow map · Asset & boundary inventory · Initial SSP · Baseline SPRS score · Gap register

02 BUILD — Engineer the controls.

Remediate technical gaps with enclave architecture, identity hardening, encryption, logging, and incident-response plumbing — then document everything.

Artifacts produced: GCC High / enclave decision · MFA + privileged access · FIPS-validated encryption · SIEM + 90-day log retention · POA&M; with owners + dates

03 TRANSFORM — Operationalize compliance.

Move from project to program: continuous monitoring, annual control testing, vendor oversight, and an executive cadence that keeps your score audit-ready year-round.

Artifacts produced: Continuous monitoring runbook · Annual control test results · Vendor risk register · Tabletop exercise reports · Quarterly SSP refresh

THE 14 FAMILIES, SIMPLIFIED

Translating 110 controls into shop-floor language

Every NIST 800-171 control rolls up to one of 14 families. The table below names each family in plain English, identifies the operational owner most manufacturers assign, and flags the highest-leverage actions.

Family	In plain English	Owner	Highest-leverage moves
3.1 Access Control	Who can touch what.	IT + HR	Role-based access · MFA · privileged account vault
3.2 Awareness & Training	Train the humans.	HR + IT	Annual CUI training · phishing drills · role-specific modules
3.3 Audit & Accountability	Log it. Review it.	IT / SOC	Centralized logging · 90-day online retention · weekly review
3.4 Configuration Mgmt	Known-good baselines.	IT	Hardened images · change control · software allowlisting
3.5 Identification & Auth	Prove who you are.	IT	Unique IDs · FIPS-validated MFA · password policy
3.6 Incident Response	Plan, practice, report.	IT + Ops	IR plan · 72-hr DoD reporting · annual tabletop
3.7 Maintenance	Safe servicing of systems.	IT + Facilities	Sanitize media · escort vendors · log maintenance
3.8 Media Protection	Drives, prints, USBs.	IT + Ops	Encrypt removable media · marking · sanitization at EOL
3.9 Personnel Security	Vet the people.	HR	Background checks · access termination on exit
3.10 Physical Protection	Locks, badges, cameras.	Facilities	Badged entry · visitor logs · alternate work-site rules
3.11 Risk Assessment	Know your exposure.	vCISO / IT	Annual risk assessment · vuln scanning · supplier risk
3.12 Security Assessment	Test the controls.	vCISO / IT	Annual SSP review · POA&M · independent assessment
3.13 System Protection	Encrypt + segment.	IT	TLS 1.2+ · enclave segmentation · DNS filtering
3.14 System Integrity	Patch + monitor.	IT	Patch SLAs · EDR · email filtering · IOC monitoring

THE 90-DAY ROADMAP

From zero to a defensible SSP in one quarter

A pragmatic sequence we use with manufacturers entering the DoD supply chain. Adjust durations to your team's bandwidth — but do not skip the order.

Days 1–15 Scope & inventory

- Define the CUI boundary (which systems, which users, which sites).
- Build a data-flow diagram showing CUI ingress, processing, storage, and egress.
- Produce an authoritative asset inventory (endpoints, servers, network gear, SaaS, OT/IIoT).

Days 16–30 Gap assessment & SPRS baseline

- Score every control YES / PARTIAL / NO against NIST 800-171A objectives.
- Calculate baseline SPRS score using the DoD scoring methodology (start: -203).
- Draft v0.1 of the System Security Plan using the inventory and scoring outputs.

Days 31–60 Quick wins & enclave decision

- Enable MFA on all remote access, email, and admin accounts (closes 5+ controls).
- Decide enclave strategy: GCC High, on-prem segmented enclave, or sovereign cloud.
- Stand up centralized logging with 90-day online / 1-year archival retention.
- Roll out FIPS-validated encryption for endpoints and removable media.

Days 61–90 Documentation, POA&M;, rehearsal

- Lock SSP v1.0 with current state, residual risk, and assessor-readable narrative.
- Publish POA&M; with named owners, target dates, and weekly stand-up cadence.
- Run an incident response tabletop covering a CUI exfiltration scenario.
- Submit refreshed SPRS score and prepare evidence binder for prime / C3PAO review.

AUDIT-READINESS CHECKLIST

What an assessor (or your prime) will ask for

If you can produce these ten artifacts on demand, you are functionally audit-ready. Missing more than three is a near-certain finding.

#	Artifact	What 'good' looks like
1	System Security Plan (SSP)	Current within 12 months · all 110 controls addressed · CUI boundary defined.
2	Plan of Action & Milestones (POA&M)	Each open control has a named owner, target date, and status.
3	SPRS score submission	Most recent score in the DoD Supplier Performance Risk System.
4	CUI data-flow diagram	Visual showing how CUI enters, flows, and leaves the environment.
5	Asset inventory	Authoritative list of in-scope endpoints, servers, SaaS, and network gear.
6	Identity & access evidence	MFA enforcement reports, privileged access reviews, JML records.
7	Logging & monitoring evidence	Sample SIEM dashboards, retention policy, weekly review records.
8	Incident response plan + tabletop	Documented IR plan and evidence of an exercise within 12 months.
9	Vendor / supply-chain risk register	Flow-down of DFARS clauses to relevant subcontractors.
10	Training records	Annual CUI / security awareness completion logs by user.

Common findings we see (and how to avoid them)

- **SSP and reality disagree.** Document the system you actually run, not the one you wish you ran.
- **POA&M with no dates.** An undated POA&M reads as 'we will never fix this.'
- **Shared admin accounts.** Each admin needs a unique ID; shared 'admin' is an automatic finding.
- **Logging without review.** 90-day retention is meaningless if no one reviews the alerts weekly.
- **OT systems out of scope.** If a CNC controller touches CUI drawings, it is in scope. Period.

NEXT STEP

Want a 30-minute audit-readiness review?

We will walk through your CUI scope, your current SPRS score, and the three controls most likely to cause a finding in your next assessment. No slides, no pitch — just a working session with a senior engineer.

Book your discovery call

trnsfrm.tech · info@trnsfrm.tech · Cleveland · Columbus

About TRNSFRM

TRNSFRM is a Cleveland- and Columbus-based managed cybersecurity and IT firm specializing in NIST 800-171, CMMC, ITAR, FTC Safeguards, ISO 27001, and HIPAA. Our IT Resilience Framework™ is the operating system we use to take manufacturers from compliance ambiguity to defensible, audit-ready operations.

Disclaimer: This guide is educational and reflects our practitioner experience. It is not legal advice and does not substitute for the official NIST SP 800-171 publications, NIST SP 800-171A assessment objectives, or DoD Assessment Methodology guidance.