TECH CON

Compliance in Motion

2025’s Biggest Regulatory Shifts & What’s Next for 2026

DON'T HAVE THE APP?

Download it here.

Scan to check-in or use code: Compliance1

TECH CON

What We'll Cover

01		**The Regulatory Landscape** *Why 2025–2026 is a pivot year*	5 min
02		**CMMC 2.0** *DoD contractors — effective November 2025*	12 min
03		**HIPAA Security Rule Overhaul** *Proposed rule taking shape in 2026*	12 min
04		**NIST AI RMF** *Governing AI risk across the enterprise*	10 min
05		**Roadmap & Q&A** *Cross-framework convergence and action plan*	6 min

WHY THIS MATTERS

Compliance Is No Longer Optional

Three regulatory shifts are reshaping how organizations across industries handle sensitive data, AI, and supply-chain risk — depending on the markets you serve, one, two, or all three may land on your program inside the same 18-month window.

220K+

DoD contractors in scope of CMMC 2.0

2026

Expected year of HIPAA Security Rule finalization

3

Frameworks reshaping the 2025–2026 landscape

The 2025 / 2026 Regulatory Timeline

NOV 2025

CMMC 2.0 Effective

32 CFR Part 170 in force; required in DoD contracts.

Q1 2026

Self-Assessments Underway

Level 1 and initial Level 2 assessments affirmed in SPRS.

Q2 2026

HIPAA Rule Finalization

OCR moves the proposed rule toward final.

MID 2026

C3PAO Audits Begin

Third-party Level 2 assessments for CUI contracts.

LATE 2026

AI RMF Integration

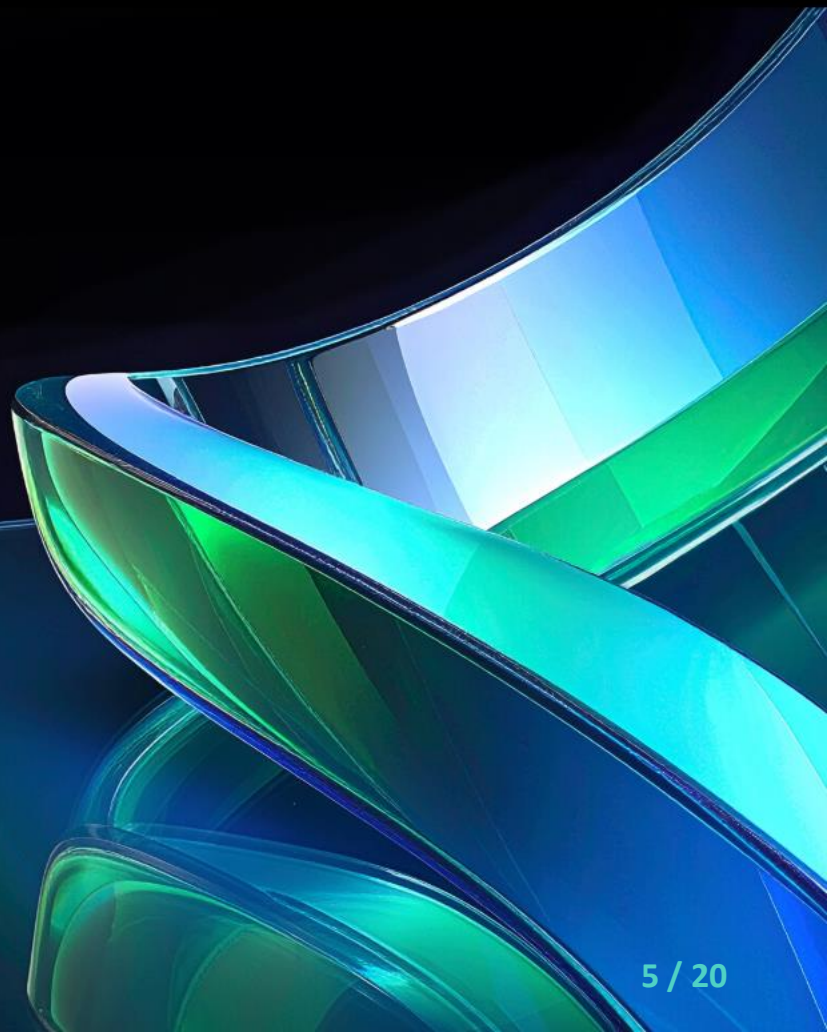
Govern / Map / Measure / Manage fold into compliance.

PART ONE

CMMC 2.0

Mandatory compliance for DoD contractors handling FCI and CUI

Effective November 2025 • Phased rollout through 2028



What CMMC 2.0 Requires

The Cybersecurity Maturity Model Certification (CMMC) 2.0 codifies cybersecurity expectations across the entire Defense Industrial Base — every contractor, subcontractor, and supplier touching federal contract information or controlled unclassified information.

- Codified under 32 CFR Part 170 — legal authority now in force
- Required in new DoD contracts and solicitations
- Flow-down obligations reach every supplier tier
- Effective November 2025; enforcement ramps through 2028

Three Certification Levels

LEVEL 1

Foundational

17

security controls

SCOPE
Contractors handling FCI

VERIFICATION
Annual self-assessment

LEVEL 2

Advanced

110

security controls

SCOPE
Contractors handling CUI

VERIFICATION
Triennial C3PAO audit (most contracts)

LEVEL 3

Expert

110 +

security controls

SCOPE
Highest-priority DoD programs

VERIFICATION
Triennial DIBCAC government-led audit

Most CIT clients land at Level 2 — that's where the heavy lift lives.

NIST SP 800-171 — The Core of Level 2

Level 2 requires full implementation of all 110 security controls across 14 families. No POA&M shortcuts for mission-critical controls.

- Access Control
- Awareness & Training
- Audit & Accountability
- Configuration Mgmt
- Identification & Auth
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System & Comms
- System & Info Integrity

14 families • **110** controls

320 assessment objectives. Every control in scope — no shortcuts.

TECH CON

Phased Rollout — What Happens When

PHASE 1 *Nov 2025 → Nov 2026*	**Self-Assessments Required** Level 1 self-assessments and Level 2 self-assessments included in applicable DoD contracts. Affirmations submitted annually in SPRS.
PHASE 2 *Nov 2026 → Nov 2027*	**C3PAO Audits Expand** Level 2 third-party certifications required for contracts involving CUI. Non-certified contractors lose eligibility for new awards.
PHASE 3 *Nov 2027 → Nov 2028*	**Level 3 Enforcement** Level 3 DIBCAC-led assessments begin for the highest-priority DoD programs and prime contracts.
PHASE 4 *Nov 2028 onward*	**Full Implementation** CMMC requirement in every applicable DoD contract. Continuous monitoring and annual affirmations become the norm.

PART TWO

HIPAA Security Rule

Overhaul

The first major rewrite in more than two decades — moving toward final in 2026

Proposed Rule published Jan 2025 • Final rule and enforcement expected 2026

PROPOSED RULE

What's Changing in HIPAA

The Office for Civil Rights is moving HIPAA's Security Rule from flexible "addressable" standards to explicit, required cybersecurity controls.

TODAY — "ADDRESSABLE"

MFA
Optional — "consider where appropriate"

Encryption
Addressable — document why, not required

Risk Analysis
Required but poorly defined

Incident Response
General "procedures" — format up to you

PROPOSED — MANDATORY

MFA
Required for all access to ePHI systems

Encryption
Required at rest AND in transit — no exceptions

Risk Analysis
Formal, documented, written — annual review

Incident Response
Formal, written plan with 72-hour restoration

"Addressable" is going away. If you can't produce written policies and evidence, you're not compliant.

MFA & Encryption Become Non-Negotiable

Multi-Factor Authentication

- Required for every access pathway to ePHI systems
- Applies to workforce, contractors, and third parties
- Phishing-resistant methods prioritized (FIDO2, tokens)
- No more "MFA for admins only" — applies to all users

Encryption Everywhere

- At rest: databases, disks, backups, mobile devices
- In transit: all channels carrying ePHI
- Current NIST-approved algorithms (AES-256, TLS 1.2+)
- Key management documented and auditable

Evidence matters. Auditors will ask for encryption configs, key rotation logs, and MFA enforcement reports.

New Documentation Mandates

Annual Asset Inventory

Every system, device, and application that touches ePHI — refreshed and reviewed at least annually.

Hardware | SaaS | Media

Network Map of ePHI

Documented diagram of ePHI flows — entry, rest, and exit. Updated when infrastructure changes.

Entry/Exit | Flows | 3rd-party

Formal Incident Response

Written procedures for detection, containment, recovery, and notification — 72-hour restoration target.

Playbooks | Tabletops | 72-hr

Documented Risk Analysis

Formal, written risk assessment reviewed annually and after any material change — not vague maybes.

Threats | Impact | Remediation

ONGOING VALIDATION

Proactive Testing & Third-Party Assurance

Annual paperwork is no longer enough. The proposed rule expects continuous proof your controls work — through adversarial testing, regular scanning, and independent validation.

Penetration Testing

ANNUAL

Adversary-simulated tests of ePHI systems to find exploitable weaknesses before attackers do.

- External, internal, app-layer scope
- Qualified independent testers
- Findings tracked to remediation
- Re-test validation of criticals

Vulnerability Scans

MORE FREQUENT

Moving from annual to continuous cadence aligned with modern threat velocity.

- Monthly authenticated production scans
- Weekly scans of internet-facing assets
- Risk-ranked results with SLAs
- Patch verification & trend reporting

Third-Party Assessments

INDEPENDENT

Formal, outside-in validation of your program and the business associates you rely on.

- Annual independent assessments
- Business Associate re-verification
- SOC 2 / HITRUST attestations
- Written agreements + control evidence

PART THREE

NIST AI RMF

Not (yet) a mandate — but the language your customers are starting to speak

Voluntary today • Showing up in vendor questionnaires and procurement reviews now

What the AI RMF Actually Is

NIST's Artificial Intelligence Risk Management Framework is a voluntary, rights-preserving playbook for organizations building, buying, or using AI. It isn't a federal mandate today — but it is rapidly becoming the language of customer due diligence.

PURPOSE

Identify, assess, and govern the unique risks AI introduces — beyond traditional cybersecurity controls.

SCOPE

Every AI use case: off-the-shelf tools, custom models, and AI features embedded in everyday SaaS.

OUTCOMES

Trustworthy AI — valid, safe, secure, accountable, transparent, explainable, fair, and privacy-enhanced.

FROM THE FIELD

MN law-enforcement vendors using AI *are now answering ~100 AI-governance questions that map directly to the AI RMF.*

The Four Core Functions

GOVERN

Culture of AI risk management

Policies, roles, accountability, and oversight across the entire AI lifecycle.

MAP

Establish context for risks

Identify AI systems, purpose, data sources, stakeholders, and downstream impacts.

MEASURE

Analyze, assess, track risks

Qualitative and quantitative evaluation of bias, drift, robustness, and security.

MANAGE

Prioritize and respond

Allocate resources, implement controls, monitor continuously, respond to incidents.

Continuous, iterative — not a one-time exercise.

Aligning AI Governance with Cybersecurity

1 Inventory Every AI System

SaaS features, copilots, custom models — if it touches your data, it's in scope.

2 Classify by Risk

Tier use cases by harm potential, data sensitivity, and decision impact.

3 Extend Existing Controls

Reuse access control, logging, change mgmt, and vendor risk workflows.

4 Write AI-Specific Policies

Acceptable use, data handling, model procurement, AI incident response.

5 Monitor Bias & Drift

Model performance and fairness metrics alongside security telemetry.

6 Train Everyone

Users, developers, procurement, legal — all touch AI risk. Not just security.

Your 2026 Readiness Roadmap

Q2 2026
Baseline & Scope

- Identify FCI, CUI, ePHI, AI systems
- NIST SP 800-171 self-assessment in SPRS
- Stand up AI inventory & use-case register

Q3 2026
Close the Gaps

- Deploy MFA universally; encrypt everything
- Formalize IR plan; run first tabletop
- Publish AI acceptable-use policies

Q4 2026
Formalize & Document

- Documented risk analyses (HIPAA + AI RMF)
- Network diagram of ePHI; inventory signed
- Board-level reporting cadence

2027+
Audit-Ready Operations

- Engage C3PAO for Level 2 certification
- Continuous monitoring across frameworks
- Annual affirmation + model-risk refresh

KEY TAKEAWAYS

01

CMMC 2.0 is live.

If you touch DoD work, self-assess now; plan for C3PAO audits in 2026.

02

HIPAA is getting teeth.

MFA, encryption, pen testing, and written plans are no longer optional.

03

AI risk is compliance risk.

Govern, Map, Measure, Manage — across every AI system in your environment.

04

Controls stack, not duplicate.

One strong control satisfies CMMC, HIPAA, and AI RMF. Build once; map everywhere.

Questions & Discussion

Nate Schmitt • Director of Cybersecurity • nate.schmitt@citsolutions.net

RAFFLE · WIN IT

TECH CON

Actual giveaway may differ in color

SESSION RAFFLE

Win Adidas Duffel Bag

Pick up at Help Desk (near registration)

GIVEAWAY COORDINATOR | TOMMY

UP NEXT

Don't miss what's next.

GRAND BALLROOM

Closing remarks & Giveaways