HORNBACK STRATEGIC SERVICES LLC

Defending the Arsenal of Democracy

THE EXECUTIVE BLUEPRINT

A CEO's Guide to CMMC 2.0 Compliance

All 14 Control Families — Through a Leadership Lens

No jargon. No IT speak. Just what every CEO, owner and founder needs to know to protect their prime contracts.

Andrew Hornback

CEO & Founder, Hornback Strategic Services LLC

CISSP • CMMC-RP • Ph.D. Candidate, Cybersecurity Leadership

hornback.us • calendly.com/andrew-hornback

HORNBACK

STRATEGIC SERVICES

A Letter from the Founder

To my fellow business leaders in the Defense Industrial Base:

National security and national defense is our family business. Generation after generation, men and women in my family have answered the call to serve — as far back as the Revolutionary War. That legacy is why Hornback Strategic Services exists, and it is the standard against which we measure our work every single day.

I wrote The Executive Blueprint for you. Not for your IT department — for you.

Over the past several months, I have published this series, one control family at a time, on LinkedIn and on our website. The response has confirmed what I already believed: leaders in the Defense Industrial Base are hungry for a plain-English guide to CMMC 2.0 that treats them as the decision-makers they are — without drowning them in acronyms or handing the responsibility off to someone in a server room.

This white paper compiles the entire series in one place.

The Cybersecurity Maturity Model Certification — CMMC 2.0 — is not an IT audit. It is a business certification. It determines whether your company can bid on, win, participate in and retain the defense contracts that pay your people and fund your growth. And the decisions that drive compliance success or failure live in the executive suite, not the server room.

If your company generates a meaningful percentage of its revenue from defense contracts, this document is not optional reading. It is the foundation of your business's future.

Read it. Mark it up. Bring it to your next leadership meeting. Then call me — I'd be glad to spend thirty minutes walking through where you stand.

We are steadfast in our commitment to protecting and defending you.

Andrew Hornback
CEO & Founder, Hornback Strategic Services LLC
CISSP • CMMC-RP • Ph.D. Candidate, Cybersecurity Leadership
calendly.com/andrew-hornback • hornback.us

What Is CMMC 2.0 — and Why Does It Matter to You?

The certification that determines your eligibility to compete in the Defense supply chain

The Cybersecurity Maturity Model Certification — CMMC 2.0 — is the U.S. Department of Defense's program to protect two categories of sensitive information flowing through the defense supply chain:

- **Controlled Unclassified Information (CUI):** Sensitive U.S. Government information that must be safeguarded but is not classified (SECRET, TOP SECRET, etc.). If a prime contractor or the DoD has ever sent you documents bearing a CUI banner marking, you handle CUI. When in doubt, assume yes.
- **Federal Contract Information (FCI):** Information provided by or generated for the U.S. Government under a contract. If you hold any defense contract, you have FCI.

CMMC 2.0 Level 2 — the minimum level applicable to DIB subcontractors who handle CUI — is built on the 110 security practices outlined in NIST SP 800-171. Compliance with these practices is becoming a contractual prerequisite to bid on, win and retain contracts. It is not optional and it is not coming slowly.

> *"For small to mid-sized businesses, the biggest risk isn't the technology; it's the lack of executive governance. You absolutely cannot delegate the survival of your company to an overworked IT manager and hope for the best." — Andrew Hornback*

The most important reframe for every executive reading this: **CMMC 2.0 is a business strategy problem, not an IT problem.** The decisions that drive compliance — who has access, how data moves, what happens in a crisis — are made in the executive suite. The technology simply reflects those decisions.

Before we walk through the 14 control families, one foundational concept requires specific attention.

Understanding CUI and FCI

The data at the center of every compliance requirement

CUI is not classified — but it is sensitive. It is U.S. Government-owned or created information that must be safeguarded and disseminated in accordance with law, regulation and government-wide policy. CMMC was created specifically to ensure that defense contractors and their suppliers protect this data with the same discipline the government requires of itself.

FCI is information that exists because of your contract with the government. You generated it for them, or they gave it to you to perform the work. It is never intended for public release — and it must be treated accordingly.

For a comprehensive listing of CUI categories and markings, see the National Archives CUI Registry: https://www.archives.gov/cui/registry/category-marking-list

> *Defining the boundary of your CUI environment — what is in scope for your CMMC assessment — is one of the most consequential and cost-controlling decisions you will make on this journey. It is a Leadership and Operations decision, not an IT configuration.*

The 14 Control Families at a Glance

A quick-reference map of every domain, the leadership question it answers and who owns it

The 14 CMMC 2.0 control families are the organizing framework of Level 2 certification. Each will be assessed by a Certified Third-Party Assessor Organization (C3PAO) when you pursue formal certification. Every control family has one thing in common: ***leadership owns the outcome***.

#	Control Family	Leadership Lens	Who Owns It
1	**Access Control**	Who has the keys?	Exec / Operations
2	**Awareness & Training**	Is your team ready?	HR / Leadership
3	**Audit & Accountability**	Where are the receipts?	Management / Legal
4	**Configuration Management**	The business blueprint	Procurement / Ops
5	**Identification & Authentication**	Digital ID cards	Security Culture / Exec
6	**Incident Response**	The fire drill	C-Suite / Legal
7	**Maintenance**	Managing third-party risk	Facilities / Vendor Mgmt.
8	**Media Protection**	Securing the physical data	Office Culture / Ops
9	**Personnel Security**	Vetting the mission	HR / Leadership
10	**Physical Protection**	The facility fortress	Facilities / Ops
11	**Risk Assessment**	The executive radar	Finance / Strategy
12	**Security Assessment**	Grading your own papers	Exec / Legal
13	**System & Comm. Protection**	The digital moat	Risk Mgmt. / IT
14	**System & Info. Integrity**	The early warning system	Quality Assurance / IT

The 14 Control Families — In Depth

What each one requires, why it matters and the leadership reality beneath the technical language

Control Family 1: Access Control

Governance Over Gatekeeping

If your IT manager is the only one who knows who has access to your sensitive defense data, you don't have a security plan. You have a single point of failure. Access Control is a business strategy that ensures your revenue stays protected by limiting who can touch the data that pays the bills.

The Executive Checklist:

- **Establish System Access:** Define exactly who receives a "key to the CUI kingdom" based on job role and documented need to know.
- **Control CUI Flow:** Track how Controlled Unclassified Information moves through your business processes.
- **Separate Duties:** Ensure no single person has the power to compromise the entire system. The person who requests access should not be the one who approves it.
- **Enforce Privileged Access:** Limit administrative rights to only the specific tasks that require them.
- **Monitor & Log:** Create an immutable record of every attempt to access sensitive areas.

The "Not Just IT" Reality — *Leadership decision*: IT can build the fence, but Leadership defines the perimeter. When a subcontractor or a new hire joins the team, it is a *management decision* to grant access. CMMC 2.0 Level 2 requires that this decision is documented, reviewed and that access is revoked the moment it is no longer needed.

Control Family 2: Awareness & Training

Training People to Protect Your Information and Your Business

You can buy the most expensive firewall in the world, but it won't stop an employee from clicking an "urgent" link in a spoofed email. In the Defense Industrial Base, Awareness and Training is about building a culture where security is everyone's job — not just the IT team's problem.

The Executive Checklist:

- **Security Awareness:** Ensure every employee understands the specific risks associated with their role. Managers must understand the risks associated with their direct reports.
- **Role-Based Training:** Provide specialized training for those with elevated access — IT administrators, incident response personnel and executives (all of them, including you).
- **Threat Identification:** Teach the team how to spot and report suspicious activity. Threat reporting must be accessible to every employee, not buried in IT.
- **CUI Handling:** Train staff on the specific legal requirements for managing defense data.
- **Documentation:** Prove that training occurred and was understood. Completion records are not optional.

The "Not Just IT" Reality — *Leadership and HR function*: If your team views security as an "IT hurdle" to get around so they can work faster, your compliance is already compromised. Leadership sets the tone that security is a non-negotiable part of the mission — and models that behavior from the top.

Control Family 3: Audit & Accountability

The Digital Paper Trail

In the world of CMMC 2.0, if you didn't log it, it didn't happen. Audit and Accountability isn't about surveilling your employees; it's about maintaining a black box for your business. When a prime contractor or a U.S. Government auditor asks for proof of security, this is the control family that produces the receipts.

The Executive Checklist:

- **System Auditing:** Ensure your systems are capable of immutably recording security events.
- **User Accountability:** Map **every** action back to a specific, identified individual. No shared accounts in the CUI environment.
- **Audit Review & Analysis:** Establish a process to actually look at the logs — not just collect them.
- **Time Synchronization:** Ensure all system clocks agree so the timeline of any event is accurate and defensible.
- **Audit Records Protection:** Make certain the logs themselves cannot be deleted or altered.

The "Not Just IT" Reality — *Management requirement*: IT can enable logging, but Leadership defines accountability. If your business processes allow for shared logins or productivity workarounds, your audit trail is broken. Every person who handles defense data must be individually identifiable and accountable for their actions — and that requires a management policy, not just a technical configuration.

Control Family 4: Configuration Management

The Blueprint for Integrity

Think of Configuration Management as the quality control function for your digital infrastructure. For small and mid-sized businesses, "configuration drift" — small, undocumented changes to settings or software that accumulate silently over time — is a serious risk. This control family ensures your business operates from a known, documented and secure baseline.

The Executive Checklist:

- **Baseline Configurations:** Create a master blueprint for how every computer, server and piece of infrastructure should be configured.
- **Change Management:** Establish and enforce a formal approval process for any change to your CUI environment before it is made.
- **Inventory Management:** Know exactly what hardware and software you own and operate. You cannot appropriately protect what you do not track.
- **Least Functionality:** Disable everything your systems do not need to do to execute the mission — hardware and software alike.
- **Software Restrictions:** Control what programs can be installed on company devices. Unapproved installations are a compliance event.

The "Not Just IT" Reality — *Procurement and Operations*: If an employee buys software on a corporate card and installs it without review, that is a Configuration Management failure — and it is a leadership accountability gap. The "order of operations" for how your business evolves its technology must be defined and enforced from the executive level.

Control Family 5: Identification & Authentication

Verifying Every Digital Identity

In the Defense Industrial Base, "I didn't know it was that user" is not a defense. Identification and Authentication is the digital equivalent of a high-security badge system: ensuring that when someone accesses your network, they are exactly who they claim to be. For an SMB, this is the primary defense against the credential theft that enables the majority of breaches.

The Executive Checklist:

- **Unique User Identification:** Every person must have their own unique account. Generic shared logins ("Admin," "ShippingDept") are prohibited in a CMMC environment.
- **Multi-Factor Authentication (MFA):** Require more than a password for all users — a code, a physical key, or a biometric. Something you know, something you have, something you are.
- **Password Management:** Enforce complexity and rotation policies that stop attackers, not just inconvenience employees.
- **Identifier Reuse:** Prevent recycling of old usernames or IDs after an employee departs.
- **Authenticator Protection:** Safeguard the credentials and MFA tokens themselves so they cannot be intercepted or shared.

The "Not Just IT" Reality — *Security Culture — set from the top*: If you, your executives or managers request exceptions to MFA because it is inconvenient, you are creating a gap that invalidates the security investment made everywhere else. Leadership must lead by example: if the CEO uses MFA every time, everyone else will too.

Control Family 6: Incident Response

The Strategic Fire Drill

A cyber incident is not a matter of if, but when. Incident Response is the cornerstone of organizational resilience — your business's ability to absorb a blow and keep operating. For a small DIB contractor, a poorly handled incident can trigger a Stop Work order from a prime. This control family ensures you have the plan, the people and the playbook to detect, contain and recover without losing your revenue stream.

The Executive Checklist:

- **Incident Handling:** Create a step-by-step playbook for what to do when a red flag appears — before one does.
- **Incident Reporting:** Document exactly who must be notified internally and externally (DoD, legal counsel, law enforcement, cybersecurity insurer) and within what timeframe.
- **Incident Testing:** Run tabletop exercises to validate the plan before a real crisis demands it. Practice is not optional.
- **Incident Monitoring:** Deploy the smoke detectors — the tools that alert your team to an intrusion in real time, not days later.
- **Response Support:** Identify your external experts (legal, forensic, insurance) in advance – know who to call, and in what order, before you need to pick up the phone. Not after the breach.

The "Not Just IT" Reality — *Crisis Management — owned by the C-Suite*: While IT handles the technical firefighting, Leadership must manage communication with the prime, navigate the legal exposure and make the business continuity decisions. You absolutely cannot delegate a crisis to a dual-hatted IT manager and expect the business to emerge intact.

Control Family 7: Maintenance

Managing the Mechanics — and the Risk They Bring

When a technician services your server room or a vendor connects remotely to patch a system, are they a helping hand or a security exposure? Maintenance isn't just about keeping the lights on; it's about ensuring that those who fix your business-critical infrastructure do not — accidentally or intentionally — walk away with your data.

The Executive Checklist:

- **Controlled Maintenance Tools:** Ensure diagnostic software and repair tools used on your systems do not carry digital hitchhikers (malware).
- **Equipment Sanitization:** Appropriately clear sensitive data from hardware before it leaves your facility for repair.
- **Media Inspection:** Inspect any storage devices brought by maintenance personnel before they connect to your systems.
- **Nonlocal Maintenance:** Require multi-factor authentication and supervisor approval or escort for any remote repair session.
- **Supervision:** Ensure unvetted maintenance staff are escorted or monitored at all times while on-site. No exceptions.

The "Not Just IT" Reality — *Facilities and Vendor Management*: IT cannot always escort the air conditioner repair technician or the copier technician around the office. Leadership must establish the policy that maintenance is a supervised activity. Procurement must ensure service contracts include the required security language before a vendor sets foot in your facility.

Control Family 8: Media Protection

Securing the Physical Data

CUI doesn't live only on your server. It can live on USB drives, external hard drives and even documents in your printer's paper tray. Media Protection is about controlling the physical objects that hold your revenue-generating defense data. If you can't account for your media, you can't account for your compliance.

The Executive Checklist:

- **Media Storage & Access:** Physically lock up all digital media and paperwork containing CUI, and limit who holds the key.
- **Media Marking:** Clearly label every drive or document that contains CUI. There is no "I didn't know" defense.
- **Media Sanitization:** Shred paper and wipe digital drives to DoD standards before discarding or reusing them.
- **Media Transportation:** Control how sensitive data moves — encrypted, locked drive carrier or secure courier. Not a personal backpack.
- **Prohibiting Portable Media:** Restrict the use of personal USB drives or unverified devices on all company systems.

The "Not Just IT" Reality — *Office Culture and Operations*: IT can disable USB ports but cannot stop an employee from leaving sensitive materials on a desk or discarding a CUI-marked document in the standard trash. Leadership must enforce clean desk policies and provide the physical tools — shredders, locked bins, secure storage — that make compliance operationally achievable.

Control Family 9: Personnel Security

Vetting Your Most Valuable — and Most Consequential — Asset

Cybersecurity isn't only about adversaries in distant locations. Threats can originate from inside your organization. Personnel Security is the process of ensuring that every person who touches your defense data is trustworthy, and that their access is actively managed throughout their entire tenure with your company. For an SMB, one poor hire or a mishandled termination can jeopardize your most profitable contracts.

The Executive Checklist:

- **Screen Individuals:** Conduct appropriate background checks for everyone before they access CUI systems — including executives. No exemptions.
- **Protect CUI During Role Changes:** Maintain security continuity during internal transfers, promotions or role changes.
- **Formal Termination Procedures:** Implement a documented, immediate "kill switch" process to revoke all access when someone leaves, voluntary or otherwise.
- **Access Revocation:** Verify that keys, badges and digital credentials are recovered or disabled at the moment of separation — not at the end of the week or whenever someone gets around to it.
- **Personnel Accountability:** Establish clear, documented links between individuals and their access authorizations.

The "Not Just IT" Reality — *HR and Leadership function*: IT cannot run a background check, and IT will not know an employee was terminated until HR communicates it. Any delay in that chain is a compliance exposure. Tight coordination between HR and IT — governed by executive policy — is the only adequate defense.

Control Family 10: Physical Protection

The Fortress Around Your Data

The strongest encryption available provides no protection if someone can walk into your office and carry off a system or a briefcase full of blueprints. Physical Protection is about securing the spaces where your defense work happens. For businesses with open-office environments or remote workers, this control family often requires a meaningful shift in culture and operations.

The Executive Checklist:

- **Limit Physical Access:** Document and use appropriate signage to mark areas where CUI is stored or processed and restrict entry to authorized personnel only.
- **Escort Visitors:** Enforce a strict policy that unvetted guests — delivery drivers, vendors, family members — are always supervised in secure areas.
- **Maintain Access Logs:** Keep a physical or digital record of everyone who enters and exits sensitive spaces.
- **Control Physical Access Devices:** Actively manage the keys, badges, and codes that unlock your facility. This includes having a process to handle lost or stolen physical access devices.
- **Secure Alternate Work Sites:** Extend physical protection requirements to home offices and remote locations where defense work is conducted.

The "Not Just IT" Reality — *Facilities and Operations*: IT doesn't install deadbolts or manage the visitor log. Leadership must decide that the back door will not be propped open for convenience, and that "working from home" carries specific, documented physical security requirements that apply equally to all employees — starting with the owner.

Control Family 11: Risk Assessment

The Executive Radar

You wouldn't fly a plane without checking the radar for storms. Risk Assessment is the radar for your business. It is the process of identifying where your vulnerabilities are before a malicious actor finds them. This is not a one-time IT task; it is a strategic leadership discipline that ensures limited resources are directed at the right defenses.

The Executive Checklist:

- **Periodically Assess Risk:** Regularly examine your operations and third-party dependencies to surface security gaps before they become breach vectors.
- **Scan for Vulnerabilities:** Use tools to find problems, open doors and other issues in your software and systems — on a defined, recurring schedule.
- **Remediate Vulnerabilities:** Close identified gaps within a reasonable, documented timeframe. Open vulnerabilities with no acceptance or remediation plan are a C3PAO red flag.
- **Update Risk Assessments:** Refresh your risk picture whenever you win a new contract, change technology or undergo significant operational change.
- **Identify Threat Levels:** Categorize risks so you can address the house fire before the leaky faucet.

The "Not Just IT" Reality — *Financial and Strategic decision*: IT can provide a list of vulnerabilities, but Leadership must provide guidance on which ones justify the investment to remediate. If your organization has no formal Risk Assessment, you are making security spending decisions on instinct. Assessors expect a Risk Assessment that is organizational in scope — not merely IT-centric.

Control Family 12: Security Assessment

Grading Your Own Papers Before the Auditor Does

There is a fundamental difference between believing you are compliant and knowing you are. Security Assessment is the internal audit that validates your controls are actually working. Think of it as a required pre-test before a Certified Third-Party Assessor Organization (C3PAO) conducts your official CMMC assessment. Finding a failure yourself and closing it is a strategic win. Failing the formal assessment is expensive.

The Executive Checklist:

- **Assess Security Controls:** Periodically review every policy and test every technical control to verify it has not degraded.
- **Develop a System Security Plan (SSP):** Create the master document describing exactly how your organization meets every CMMC requirement. CRITICAL: Without an SSP, you will automatically fail your C3PAO assessment.
- **Create Plans of Action & Milestones (POA&M):** Document precisely how and when remaining security gaps will be closed. Open gaps without a plan are unacceptable. CRITICAL: Controls worth 5 points and most worth 3 points must be implemented prior to a C3PAO assessment.
- **Monitor Security Controls:** Maintain ongoing observation to ensure your team is not cutting corners under operational pressure.
- **Review System Boundaries:** Confirm CUI remains within your defined secure perimeter. If it extends beyond that boundary, your scope and all related documentation must be updated.

The "Not Just IT" Reality — *Executive ownership — no delegation*: The System Security Plan (SSP) is one of the most important documents in your CMMC journey, and it must be signed by Leadership. IT provides the technical details, but the executive team owns the commitment. If the SSP does not match operational reality, the liability falls on the executive team — not the IT manager.

Control Family 13: System & Communications Protection

Defending the Digital Perimeter

Consider that your business is a castle, System and Communications Protection is the moat, the drawbridge and the guards on the wall. For a DIB subcontractor, having a firewall is not enough. You must prove that the channels through which your contracts, blueprints and sensitive data travel are locked down tight. This is the infrastructure that guarantees data entrusted to you by the U.S. Government or a prime will not reach unauthorized hands.

The Executive Checklist:

- **Boundary Protection:** Monitor and control communications at your network perimeter — blocking unauthorized traffic at the point of entry.
- **Public vs. Private Separation:** Digitally separate your internal work environment from public-facing services like your corporate website.
- **Cryptographic Protection:** Apply FIPS-validated encryption to CUI whether it is in motion (being transmitted) or at rest (being stored).
- **Deny by Default:** Configure systems to block all traffic except what is explicitly required for business operations.
- **Secure Name Resolution:** Protect your DNS infrastructure so employees are not redirected to malicious sites through your own network.

The "Not Just IT" Reality — *Risk Management decision*: IT can implement the deny-all rule, but Leadership must define and approve the exceptions. If your organization permits shadow IT — employees using unapproved messaging apps, file-sharing services, or personal devices — you are creating uncontrolled pathways for CUI to leave your environment. That is a leadership accountability gap, not an IT failure.

Control Family 14: System & Information Integrity

The Early Warning System

In high-stakes defense contracting, the absence of alerts is not a guarantee of safety. System and Information Integrity is about ensuring your data remains accurate and your systems remain healthy. This is your organization's immune system — the capacity to detect corruption or unauthorized modification and neutralize it before it destroys your reputation or your revenue.

The Executive Checklist:

- **Flaw Remediation:** Identify and patch security holes in your software before adversaries exploit them. Patch schedules are not optional and compliance must be documented.
- **Malicious Code Protection:** Deploy and actively maintain anti-malware tools that generate alerts when threats are detected.
- **System Monitoring:** Maintain continuous visibility into your network to identify anomalous behavior as it happens.
- **Security Alerts:** Ensure that when something goes wrong, the right people are notified immediately — not discovered weeks later by accident.
- **Software & Information Integrity:** Verify that sensitive data has not been secretly altered or corrupted.

The "Not Just IT" Reality — *Quality Assurance priority*: If your dual-hatted IT staff are too consumed with daily operations to apply critical patches, your standing as a trusted defense partner is eroding in real time. Leadership must build maintenance time into the operational calendar and treat it as a non-negotiable priority — not something that happens when things slow down.

The Pop Quiz

14 questions every DIB executive should be able to answer with confidence

Before you submit your next defense bid, before you pursue CMMC certification and before you assume your compliance program is in order — answer these questions honestly. They map directly to the 14 control families above.

- **Access Control:** Is your overworked IT manager making access decisions that should come from the executive suite?
- **Awareness & Training:** Is your organization relying on luck instead of a structured training program to protect your data, your prime's data and the U.S. Government's data?
- **Audit & Accountability:** Are your systems producing accurate, complete logs that would satisfy a government auditor's scrutiny?
- **Configuration Management:** Is your IT environment a Wild West of undocumented changes?
- **Identification & Authentication:** Are your digital ID badges easy to forge or share?
- **Incident Response:** Has your incident response playbook been tested within the past year?
- **Maintenance:** Is your open-door policy for repair crews creating an unguarded entry point for adversaries?
- **Media Protection:** Do your employees know how to physically secure CUI — in the office, in transit and when working remotely?
- **Personnel Security:** Are your onboarding and offboarding processes fully CMMC-compliant?
- **Physical Protection:** Could someone — friend or adversary — walk into your server room unchallenged?
- **Risk Assessment:** Is your security posture built to address today's threats or yesterday's?
- **Security Assessment:** Does your organization have a signed System Security Plan that reflects current operational reality?
- **System & Communications Protection:** Is your digital drawbridge left open for the sake of convenience?
- **System & Information Integrity:** Does your organization's immune system have the strength to withstand a targeted, advanced persistent attack?

> *Any answer that gives you pause is a gap a C3PAO assessor will find. Finding it yourself — and closing it with a documented remediation plan — is the difference between a clean assessment and a failed one.*

Your Next Step

Compliance is not the finish line — it is the foundation

CMMC 2.0 compliance is not a one-time project. It is an ongoing operational commitment. The organizations that treat it as a strategic business function — rather than a regulatory burden to endure — are the ones that win and retain the contracts that matter.

Hornback Strategic Services was built to be your partner at every stage of that journey. We are a U.S.-based firm comprised entirely of U.S. citizens, with CMMC Registered Practitioners on staff, a CISSP-certified leadership team and over 30 years of combined information security experience across defense, government, manufacturing, transportation, higher education, pharmaceutical and commercial sectors.

We do not sell products, period. We do not maintain vendor relationships that influence our recommendations. We are vendor-agnostic, relationship-driven consultants who work alongside your team to build compliance programs that are sustainable, scalable and integrated into your business strategy — not bolted on as an afterthought.

Our Four Service Pillars:

I. The Compliance Engine	CMMC Scope Analysis & Assessment, Gap Analysis & Remediation, Strategic Roadmap Development
II. Strategic Governance	Fractional CISO Leadership, Information Security Strategy & Architecture, Gap Assessment (NIST, CMMC, ISO)
III. Resilience & Continuity	Business Impact Analysis, Incident Response & Disaster Recovery Planning, Tabletop Exercises, Risk Assessment
IV. Tactical Support & Remediation	Strategic Remediation Support, Documentation Creation & Review, General Cybersecurity Consulting

Schedule Your Complimentary CMMC Strategy Call

30 minutes. No sales pitch. An honest assessment of where you stand.

calendly.com/andrew-hornback • hornback.us

Hornback Strategic Services LLC — Defending the Arsenal of Democracy