ebook

MISSION-CRITICAL CYBERSECURITY:

Aligning Defense Resources in the Digital Battlespace

A Strategic Framework for Defense Leaders

SPA
SYSTEMS PLANNING & ANALYSIS

Contents

THE EVOLVING CYBERSECURITY IMPERATIVE

Cybersecurity is no longer a back-office function. In today's digitized battlespace, it has become a cornerstone of national defense strategy. Sophisticated cyber threats now span both military and civilian infrastructure, requiring defense leaders to confront how best to safeguard critical systems while optimizing limited resources.

The question is no longer whether to invest in cybersecurity—but how to prioritize those investments for the greatest mission effect.

This insight captures a core dilemma: complete security is cost-prohibitive and often counterproductive. Cyber resilience requires making tough, mission-informed trade-offs.

A Strategic Reframing for the Department of Defense

Cybersecurity must now be treated as a foundational element of warfighting. This shift represents:

- → An opportunity to operationalize cybersecurity thinking
- → A reframing of risk as mission degradation—not just data compromise
- → A strategic advantage amid persistent digital conflict

This ebook offers senior defense leaders a practical framework for informed decision-making, based on field-proven expertise and SPA's mission-focused cyber assessments.

> **It's one thing to try to make something completely impervious to cyber assault, but you probably can't afford that.**
>
> – **Mike Farren,** Strategic Growth and Business Analyst at Systems Planning & Analysis (SPA)

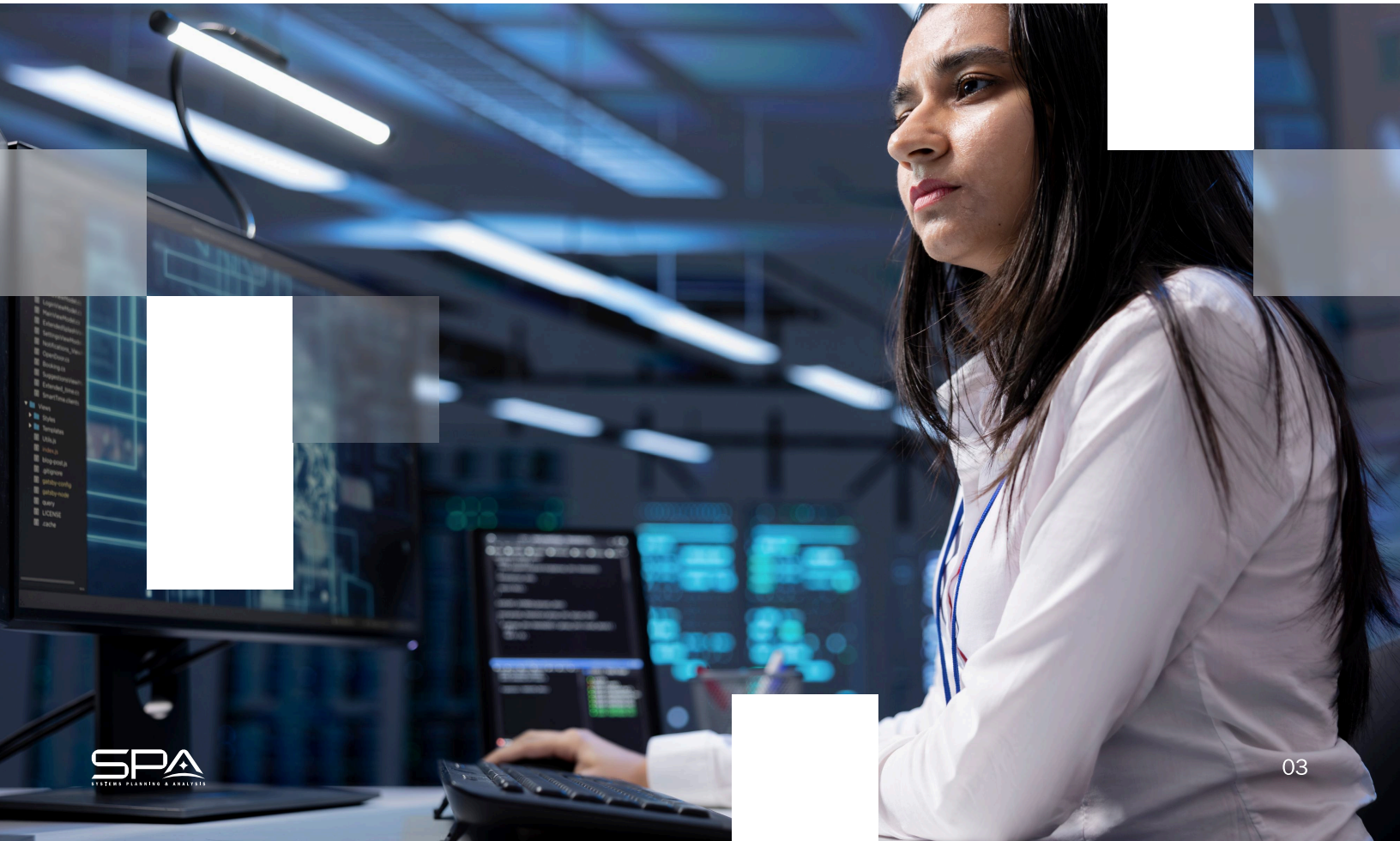
MOVING BEYOND COMPLIANCE: CYBERSECURITY AS STRATEGIC ENABLER

Cyber investments must do more than meet audit requirements—they must serve the mission.

For the defense industrial base (DIB), this principle has operational consequences. Many DIB contractors are small businesses with constrained cybersecurity resources. For example, protection levels often fail to reflect mission importance and true prioritization means aligning defense-wide cybersecurity efforts with mission impact.

The Limits of CMMC

While the Cybersecurity Maturity Model Certification (CMMC) aims to tier requirements, Farren notes its misalignment: “It tends to be tied to the sensitivity of the CUI [Controlled Unclassified Information] data, not to the mission that data supports. That’s where DoD still struggles—deciding where the next cyber dollar should go.”



The Alignment Challenge

We don’t do cyber for cyber’s sake. We do it because a critical DoD mission needs to be accomplished.

Mission-Informed Resource Strategy

By anchoring cybersecurity decisions in mission objectives, defense leaders can:

1. Focus protection on critical operational nodes
2. Justify investments using mission degradation risk
3. Move from reactive compliance to proactive resilience
4. Ensure cyber spend supports defense readiness, not just audits

Strategic Question:

How are your current cyber investments reinforcing your most vital operational outcomes?

✦ Case Study

NotPetya and the Cost of Misaligned Priorities

Global Spread: Initially targeted Ukraine, but escalated

Impact: >$300M in damages to Maersk; serious disruption at Merck

Defense Link: Ripple effects across logistics chains supporting defense missions

Key Lesson: Peripheral system breaches can create front-line operational failure

VISUALIZING MISSION DEPENDENCIES: THE MISSION STACK

Cyber vulnerabilities don't occur in isolation. The mission stack framework equips defense leaders to map cyber risk across the full operational ecosystem—from tactical systems to civilian infrastructure.

The Mission Stack Framework

Originating from the Cyber Warfare Directorate within the Office of the Deputy Secretary of Defense, this layered model visualizes how a disruption at any tier can cascade into mission failure.

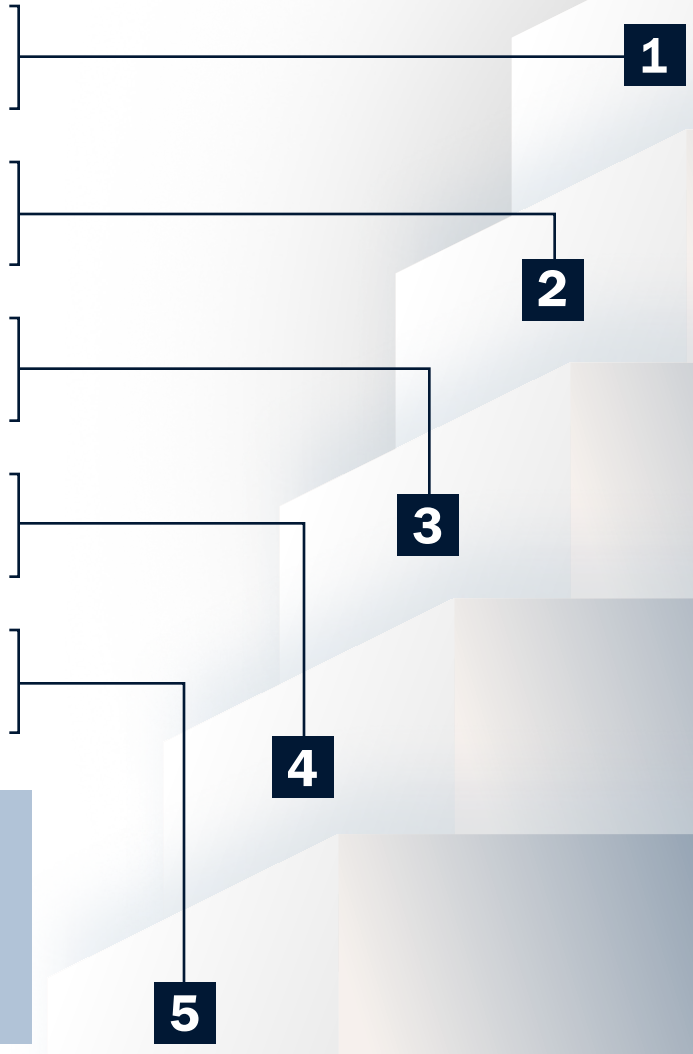
Mission Systems – Warfighting platforms, C2 systems, tactical communications

IT/Network Infrastructure – Enterprise networks, data centers, authentication layers

Facilities Infrastructure – Bases, utility control, support logistics

Commercial/Civilian Infrastructure – Power, telecom, transportation

Supply Chain – Hardware sourcing, software dependencies, vendor integration



SPA assessments have shown a persistent imbalance: security measures are concentrated at the top of the stack, leaving lower tiers exposed.

Cross-Domain Vulnerabilities

Defense leaders face a persistent jurisdictional challenge:

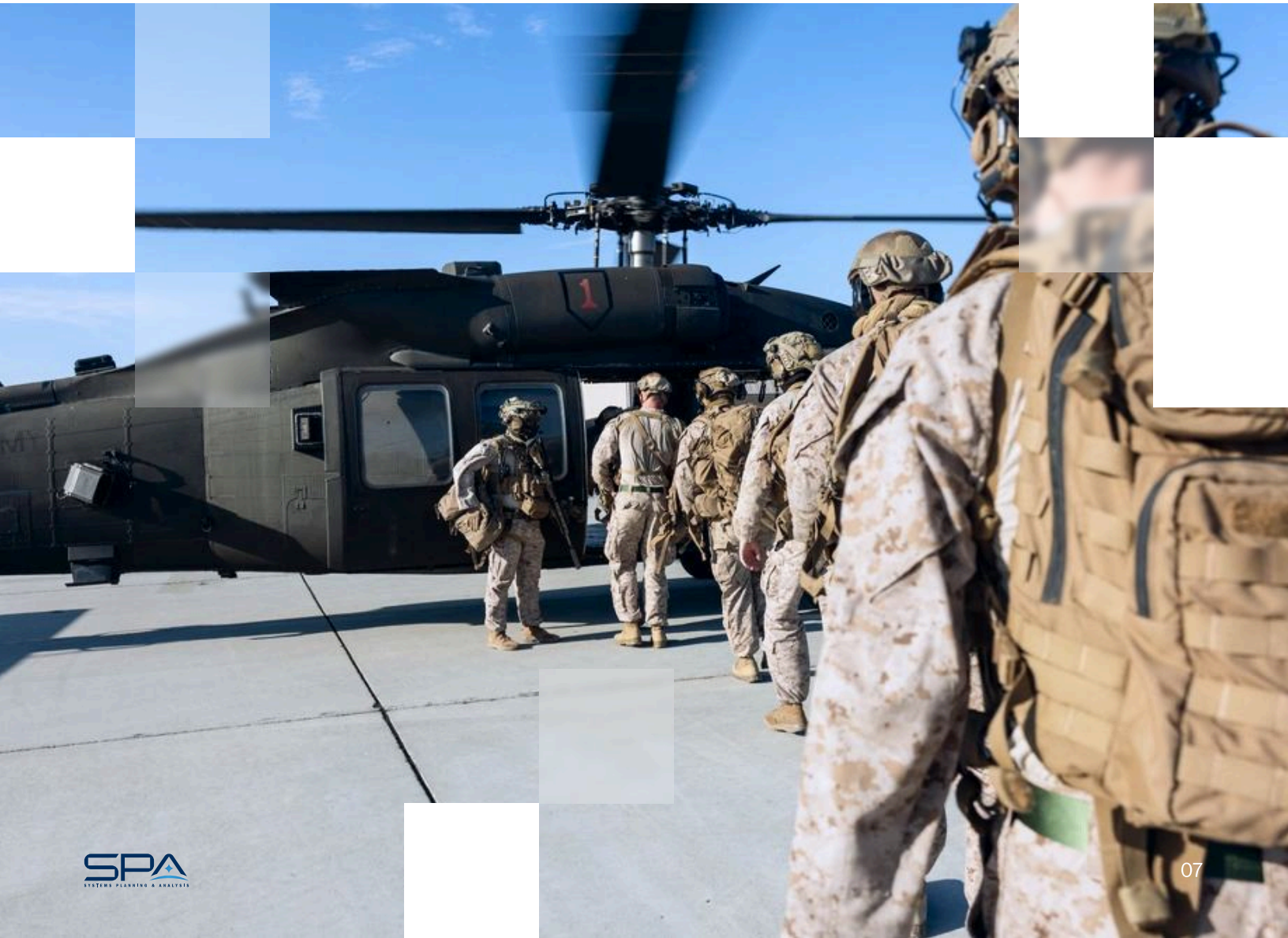
→ DoD authority is strongest over direct military assets

→ Critical enablers often lie outside that boundary

→ True cyber defense requires agency-to-agency integration

Farren says, “When you dig below the 65,000-foot level, you discover cybersecurity vulnerabilities that weren’t fully understood—and how they impact whether a very expensive, very important weapon system actually leaves the rail.”

By embracing the mission stack perspective, leaders can shift from asset-based defense to mission-centric cyber assurance.



An effective cyberattack at any level of the mission stack can compromise the mission.

A power substation disruption, a telecommunications breach, or a supply chain vulnerability can render the most sophisticated weapon system inoperable—or worse, undetectably degraded.

ORGANIZING FOR CYBER EFFECTIVENESS: STRUCTURAL AND STRATEGIC LEVERS

To defend against dynamic cyber threats, the Department of Defense must continuously refine how cyber capabilities are structured, staffed, and aligned with broader operational goals.

Today, each service branch manages its cyber personnel independently. This approach preserves flexibility but creates challenges in standardization, joint operations, and unified response.

Yet despite progress, cyber often remains siloed—treated more as an IT function than as a domain of warfighting.

The Marginalization Gap

Even with formal recognition as the fifth warfighting domain, cyber is often subordinated to technical directorates. Assignments typically fall under J6 (communications and networks), rather than J3 (operations). This disconnect hinders real-time integration with combat planning and mission execution.

“In many cases,” Farren explains, “cybersecurity and cyber defense are assigned to J6. But we’d never delegate defensive counter-air missions to J6—yet that’s what we’re doing with cyber.”

> **Since the establishment of U.S. Cyber Command, they’ve been trying to standardize the manning, training, and equipping of a Cyber Mission Force, which is approximately 6,000 billets for offensive and defensive cyberspace operations.**
>
> – **Mike Farren,** Strategic Growth and Business Analyst at SPA

Toward Organizational Alignment

Several trends suggest momentum toward greater centralization, including potential Congressional support for a distinct cyber force. “It really is a political decision at the end of the day,” Farren observes. “But given the appetite of U.S. Cyber Command and growing Congressional direction, we’re likely to see a separate cyber force within the next three to five years.”

Key Considerations for Structural Evolution:

→ Assess integration with traditional warfighting functions

→ Design support elements for cyber forces that match kinetic mission enablers

→ Centralize selectively, preserving adaptability while improving coordination

Ultimately, any organizational structure must serve one goal: ensuring cyber capabilities are aligned directly with mission-critical objectives—not isolated from them.

BUILDING RESILIENCE ACROSS THE DEFENSE INDUSTRIAL BASE

Cyber readiness extends beyond the Department of Defense itself. The sprawling defense industrial base—especially its small business members—plays a vital role in supporting mission-critical capabilities yet remains unevenly protected.

The Small Business Challenge

Many DIB companies operate with razor-thin margins, making sustained cybersecurity investment difficult.

- → Small businesses typically spend just 0.3% of annual revenue on cybersecurity
- → A $10 million firm might afford 1–2 cybersecurity professionals—often insufficient to secure sensitive systems

Farren summarizes the dilemma: “Expecting small companies to invest upfront in securing networks to compete for contracts they may not win—that’s a hard sell. A couple of people just aren’t a viable cybersecurity team.”

> **One of the interesting bits of feedback we got from industry sectors was, ‘Thanks—but no thanks.’ Because what they find is when someone offers them something free, their regulators find out about it, and suddenly it becomes mandatory – and a financial burden.**
>
> – **Mike Farren,** Strategic Growth and Business Analyst at SPA

Federal Support Programs

To address these structural vulnerabilities, several government initiatives provide education, intelligence sharing, and technical assistance.

✦ **CISA Joint Cyber Defense Collaborative (JCDC)**	→ Real-time information sharing → Coordinated incident response → Best practice dissemination
✦ **FBI INFRAGARD**	→ Public-private threat awareness → Networking and sector collaboration
✦ **NSA Cyber Collaboration Center**	→ Penetration testing and advisory services → Technical support for cyber hygiene
✦ **DC3/DCISE**	→ DIB-specific threat intelligence → Forensics and mitigation tools

Four Levers to Improve DIB Cyber Resilience

SPA recommends practical, mission-aligned strategies that strengthen defense sector resilience without overburdening small firms:

---

01 **Incentivize Adoption**

- → Offer tax credits and contract-based rewards for exceeding baseline requirements
- → Offset upfront costs with targeted subsidies

---

02 **Simplify Compliance**

- → Harmonize reporting framework
- → Clarify phased compliance roadmaps

---

03 **Boost Intel Sharing**

- → Use simplified, secure portals
- → Push actionable alerts, not just static information

---

04 **Resource Appropriately**

- → Base expectations on mission impact, not just organization size
- → Define clear performance metrics and right-size security obligations

Cybersecurity across the DIB should no longer be a technical afterthought—it's a critical component of national defense. As Farren emphasizes, “Cybersecurity is not just about compliance—it's fundamentally about mission assurance.” The future of national security depends on our ability to view cyber defense as an integrated, strategic imperative.

STRATEGIC EXECUTION: A UNIFIED FRAMEWORK FOR CYBER READINESS

To move from reactive defense to proactive assurance, defense leaders need a unified, mission-focused framework for cyber readiness. This includes reframing how cyber integrates into operations, planning, and leadership.

Bridging Conceptual Divides

Cyber warfare differs fundamentally from kinetic warfare in that:

→ Effects are harder to predict

→ Targets evolve rapidly

→ Commercial vendors control the terrain

Farren explains: “Whether you're a surface warfare officer or a tank driver, you understand kinetic weapons. We can model the effects of a 2,000-pound bomb. We know exactly how much they cost. We know exactly the penetration against a particular target, and we understand the site or the adversary's countermeasures.

For a cyber weapon, we don't. It really is hard. The adversary is constantly changing their networks. What works on one type of operating system doesn't work on another, and unlike the kinetic world, Microsoft and other commercial providers are defending the very targets that we're trying to hit because we're all using the same COTS technologies.

This uncertainty can cause commanders to disengage. They’ll say, ‘I don’t have time to understand cyber,’ and it gets marginalized.”

Kinetic vs. Cyber Weaponry

	Kinetic Weapon e.g., GBU-31	Cyber Capability
✦ **Predictability**	High (known effects)	Variable (changing targets)
✦ **Cost Certainty**	Well-established	Highly variable
✦ **Target Stability**	Relatively static	Constantly evolving
✦ **Effect Measurement**	Clear and observable	Often ambiguous
✦ **Countermeasures**	Well-understood	Rapidly evolving

Strategic Alignment Process

A step-by-step model for aligning cyber strategy with mission impact:

---

01 **Identify Critical Missions**

- → Define essential operational capabilities
- → Establish clear priority tiers
- → Document success requirements

---

02 **Map Mission Dependencies**

- → Trace through full mission stack
- → Identify critical nodes and connections
- → Document external dependencies

---

03 **Assess Vulnerability**

- → Analyze potential compromise effects
- → Quantify operational degradation
- → Establish recovery timelines

---

04 **Allocate Resources Based on Mission**

- → Prioritize highest mission value protections
- → Balance preventive and recovery investments
- → Establish clear performance metrics

---

05 **Continuous Adaptation**

- → Regular reassessment of threat landscape
- → Adjustment to changing mission priorities
- → Evolution of protection strategies

This structured approach ensures cybersecurity is a driver of mission assurance—not an isolated technical objective.

KEY TAKEAWAYS FOR DEFENSE LEADERS

01 **Prioritize by Mission Impact**

- → Align cybersecurity investments with operational value
- → Focus on systems where failure equates to mission failure

02 **Integrate Across the Mission Stack**

- → Identify and protect critical dependencies at every layer
- → Address overlooked risks in infrastructure and supply chains

03 **Embed Cyber in Operations**

- → Elevate cyber from support role to operational necessity
- → Position cyber teams alongside warfighting elements

04 **Support the Entire Ecosystem**

- → Enable small DIB partners with practical, scalable frameworks
- → Balance compliance demands with viability and performance

05 **Lead Collaborative Defense**

- → Break jurisdictional silos between agencies and sectors
- → Build collective resilience through shared intelligence and action

Adversaries are moving quickly in cyberspace. Ensuring defense readiness in this environment demands a strategic, coordinated, and mission-centered approach—one where cybersecurity protects outcomes as well as systems.

Cybersecurity is not just about compliance—it's fundamentally about mission assurance.

TAKE THE NEXT STEP

SPA's cybersecurity and mission assurance experts stand ready to help your organization tailor and implement a cyber strategy aligned with your operational priorities.

Contact us today to schedule a consultation.

SPA and Cybersecurity

Systems Planning and Analysis (SPA) has achieved certification for Cybersecurity Maturity Model Certification (CMMC) Level 2. This requires organizations to implement and maintain a robust set of security practices aligned with the National Institute of Standards and Technology (NIST) SP 800-171, ensuring that federal contract information and CUI are protected against evolving cyber threats. SPA's successful assessment was conducted by a Certified Third-Party Assessment Organization (C3PAO) authorized by the Cyber AB.

SYSTEMS PLANNING & ANALYSIS

SCHEDULE A CONSULTATION

Contact us ↗

ABOUT SPA

For more than 50 years, SPA has been a premier, independent global provider of data-driven analytical insights advancing national security for Defense, Intelligence, and Homeland Security clients. We deliver innovative strategies and approaches for solving national security challenges with mission-specific tools and deep subject matter expertise across all domains. From policy support to program management, cloud and cybersecurity, systems engineering and AI/ML, SPA delivers unbiased, objective analysis, tailored exclusively to our clients' needs. Our operational and analytics expertise has supported multi-domain force modernization and safeguarded the nation's nuclear deterrent.

Founded on principles of objectivity, responsiveness, and trust, SPA shapes national security policies, guides acquisition programs, and ensures operational readiness. Our diverse team of seasoned professionals delivers data-driven insights that drive mission success and prepare our clients to meet both current and future challenges.

SPA is a portfolio company of Arlington Capital Partners.