G2OPS® Smarter Intelligence.®

G2 Ops Launches Cyber Ready Center of Excellence

Virginia Beach, VA, USA (17 July 2025) | Dean Smith, Vice President of Security Engineering and Enterprise Integration – The Department of the Navy (DoN) has made clear that cybersecurity can no longer be a compliance afterthought. In a strategic shift that is reshaping how systems are acquired and secured, the Navy has called for cybersecurity to be embedded from the outset—integrated into engineering practices and continuously aligned with operational risk. This transformative approach is known as **Cyber Ready**.

The question for programs is no longer whether they should adopt Cyber Ready; it is how quickly and effectively they can get there.

Institutionalizing Cyber Ready at Scale

To support this shift and accelerate adoption across the defense community, G2 Ops has launched the Cyber Ready Center of Excellence (CoE). This internal hub is dedicated to formalizing the company's delivery methods, ensuring consistent execution across teams, and driving continued innovation in secure system development.

The CoE plays a central role in how G2 Ops supports customers and partners working to operationalize Cyber Ready principles. Its objectives include:

- Delivering high-quality, mission-aligned outcomes.
- Embedding continuous cybersecurity across engineering and security teams.
- Enabling scalable growth through repeatable practices and playbooks.
- Advancing innovation in secure, model-based engineering and automation.
- Leading strategic alignment with evolving Department of Defense (DoD) and Navy cybersecurity guidance.

With the CoE, G2 Ops is strengthening its position as a trusted partner in implementing Cyber Ready frameworks across complex, security-critical environments. The CoE ensures our customers benefit from standardized best practices, experienced practitioners, and tools purpose-built to meet today's cybersecurity challenges.

What Is Cyber Ready?

Cyber Ready is a mission-aligned, risk-informed approach to cybersecurity that integrates seamlessly with system engineering, acquisition, and operations. It moves beyond checklist compliance to focus on delivering resilient, secure capabilities that can withstand adversary action in dynamic environments.

Cyber Ready emphasizes:

- Proactive risk engineering integrated from day one.
- Live, continuously updated evidence of cyber posture.
- Mission-focused risk understanding rather than static security state.
- Alignment across engineering, architecture, security, and operations.

Rather than treat cyber as an isolated phase or control set, Cyber Ready ensures cybersecurity is a persistent and measurable component of system readiness.

> "Instead of a compliance mindset, the DON will shift to Cyber Ready, where the right to operate is earned and managed every day."
>
> *DoN Cyber Strategy November 2023*

How Cyber Ready Differs from RMF

While the Risk Management Framework (RMF) remains the foundation of federal cybersecurity, Cyber Ready represents a modernized evolution of that approach. Traditional RMF often emphasizes point-in-time artifacts and documentation. In contrast, Cyber Ready focuses on continuously earned trust based on real-time mission risk.

Characteristic	Traditional RMF	Cyber Ready
Purpose	Compliance certification	*Operational cyber resilience*
Assessment	Static, point-in-time	*Continuous, risk-informed*
Artifacts	Standalone documents	*Integrated engineering evidence*
Focus	Control completion	*Mission impact and threat alignment*
Cadence	Periodic reviews	*Ongoing awareness and updates*

How G2 Ops, Inc. (G2 Ops) Enables Cyber Ready

G2 Ops' capabilities naturally align with the Cyber Ready BOE and the principles outlined in DoN guidance. Our engineering-driven approach, combined with advanced tooling and repeatable delivery methods, accelerates the path to Cyber Ready Authorities to Operate (ATOs) and strengthens system security across the lifecycle.

G2 Ops has successfully completed Cyber Ready pilot efforts that resulted in risk-based ATOs for Navy systems. These efforts demonstrate that mission-aligned cybersecurity—grounded in digital engineering—can deliver not only compliance, but real assurance. Today, G2 Ops is supporting additional systems pursuing Cyber Ready ATOs and actively partnering with other programs and SYSCOMs to plan new pilot efforts.

Alignment with Cyber Ready BOE Requirements

The Cyber Ready initiative gained significant momentum following the release of the Cyber Ready Acquisition Integration Initiative Guidance, which defined the minimum Body of Evidence (BOE) required to support risk-based ATO decisions. This guidance marked a major departure from document-heavy, point-in-time certifications, emphasizing instead real-time awareness, engineering integration, and continuous evaluation. The Navy's first Cyber Strategy later cemented Cyber Ready as a core element of the Department's cybersecurity vision.

G2 Ops delivers comprehensive support across all components of the Cyber Ready BOE:

- System technical design.
- Impact of vulnerability exploitation on system components and mission functions.
- System and Defense in Depth (DiD) architecture diagrams.
- Additional evidence, including vulnerability documentation and mission impact traceability.

These outcomes are enabled by a tightly integrated suite of tools, models, and engineering methods that operate across domains to ensure accuracy, consistency, and mission alignment.

Model-Based Systems Engineering (MBSE)

G2 Ops integrates cyber requirements and risk analysis directly into MBSE workflows to support traceability, compliance, and real-time decision-making. Cyber artifacts are derived from authoritative, system-linked models.

SOFIA

G2 Ops' mission-based assessment platform enables tailored cyber scoring, prioritization, and impact analysis. Strategic Optics for Intelligent Analytics (SOFIA) delivers non-ACAS risk computation that reflects operational context and supports continuous monitoring.

Monarch

This custom modeling environment streamlines the creation and update of cybersecurity-enabled models. Monarch accelerates the production of artifacts aligned with the Cyber Ready BOE and supports agile system changes.

Security-Focused Engineering Services

G2 Ops' approach to Cyber Ready is grounded in the integration of cybersecurity across every phase of system engineering. G2 Ops delivers a comprehensive suite of security-focused services that drive measurable risk reduction and mission assurance:

- Cybersecurity architecture and systems engineering to embed risk considerations into design.
- Residual risk and threat-informed assessment tailored to mission priorities.
- Standardization of security modeling and digital engineering practices across engagements.

This blend of technical depth, cybersecurity rigor, and digital traceability positions G2 Ops to deliver security engineering that is both repeatable and resilient. It forms the foundation for Cyber Ready success.

Ready to Take the Next Step?

Cyber Ready is not simply a better way to meet compliance; it's the *right* way to build and field systems in the face of modern threats. G2 Ops has the manpower, tools, and experience to help you deliver secure, mission-aligned capabilities from day one.

Contact us (robert.alley@g2-ops.com) to learn how G2 Ops can support your Cyber Ready journey. Whether you are planning a pilot, building your BOE, or preparing for a risk-based ATO, G2 Ops is ready to help you get there.