GATOR

Cyber Training & Readiness Platform

From "We Trained" to "We're Mission-Ready"

Commander-Focused Cyber Readiness Solution

Cold Open: Unknown Readiness Is a Risk

"If we had to fight tonight, can you prove your cyber teams are ready?"

> **The Problem:** GAO has repeatedly found DoD lacks clear, domain-level readiness metrics and reporting—especially in **cyber**.

What this means for commanders:

- Can't quantify "ready or not" beyond local proxies
- No standardized truth data across units
- Readiness reporting relies on anecdotes, not evidence

Punch-in stat: Independent analysis argues CMF training shortfalls are largely training/measurement issues and have persisted since standards were established.

Source: Government Accountability Office (GAO-23-106673) | War on the Rocks

Problem: Three Gaps That Keep Commanders Guessing

Standards Drift & Churn

USCYBERCOM’s JQR/JCT&CS cycle updates continuously (annual review; J7 notifies Services)—units chase a moving target.

Subjective Evaluation

Air Force runs **ESAP** program to police examiner standardization—because objectivity varies at squadron level.

⚡ Speed-of-Change Gap

Threats, tools, and TTPs outpace static syllabi. DoD continues to push for better measurement & software/cyber metrics.

> Current ranges lack realism, evaluations are manual/biased, and reporting isn't standardized or predictive.

Sources: USCYBERCOM GitLab (JQR) | e-Publishing (ACCI17-202v2) | DefenseScoop

Market Reality: We Train, But Can’t Verify Effects

PCTE: Necessary But Not Sufficient

- Provides maneuver space and distributed access
- Cybercom pushing toward *more complex, realistic actors*
- Acknowledges the realism gap

The platform exists—measurement at speed is the bottleneck.

Scale Is Big

6,000+

CMF Operators

PCTE supports thousands of operators—but training completion ≠ readiness proof.

Sources: PEO STRI (PCTE Program) | go.ratio.exchange | DefenseScoop

GATOR Thesis

From "I Think" to "I Know"

"We trained" → "We're mission-ready" **with evidence**

Objective Grading

Doctrinal evaluation of free-form operator inputs

Live, Adaptive Ranges

Environments that evolve with the operator

Readiness Analytics

Tied to roles & JQRs for commander truth data

How GATOR Works: Operator to Commander Loop

1. Environment Generation

Living cyber ranges reacting to mission role and actions

- ✓ Saves environment-authoring hours
- ✓ Threat-informed scenarios
- ✓ Adaptive difficulty

→

2. AI Evaluator

Doctrinal, "by-the-book," **bias-reduced grading** with instant feedback

- ✓ Supports no-notice/requal
- ✓ Aligned to Stan/Eval
- ✓ Objective rubrics

→

3. Automated Reporting

Auto-captures against latest **JQRs**; surfaces predictive gaps

- ✓ Real-time dashboards
- ✓ Training prescriptions
- ✓ Trend analysis

Result: Commanders get defensible readiness data, operators get instant feedback, and units stay aligned to current standards.

What Commanders Get: The "Why Buy" in 90 Seconds

Defensible Readiness Picture

- Per role, team, and mission set
- Not anecdotes—**objective data**
- Exportable to JCC2-R or unit systems
- Audit trail for inspections

⚡ Faster OODA Loop Close

- Instant AARs—no 2-week delays
- Trend dashboards showing proficiency deltas
- Predictive gap analysis
- Time-to-complete metrics

⚖ Comparability Across Squadrons

- Standardized rubrics + reference sets
- RBAC controls for examiner consistency

90%

Target Rubric Agreement Rate

Note: USCYBERCOM TASKORD 23-0029 designates JCC2-R as readiness system of record—GATOR can feed it.

Security & Deployment: Built for the Mission Set

Enclave-First Architecture

Model-Agnostic Design:

- On-prem LLMs (e.g., Ollama class)
- Disconnected labs supported
- SIPR/JWICS compatible
- Controlled cloud with ATO

No External Dependencies:

- Self-contained inference
- Air-gap capable
- Local model hosting

Compliance Posture

Security Controls:

- Role-Based Access Control (RBAC)
- Complete audit logs
- No student PII retention
- Encrypted data at rest & in transit

Deployment Options:

- On-premises datacenter
- FedRAMP/IL cloud (with hosting ATO)
- Tactical edge (disconnected)
- Hybrid configurations

Bottom line: GATOR deploys where you train—from unclass labs to JWICS enclaves—with mission-appropriate security

Differentiators vs. Ranges & Commercial Courses

Capability	Traditional Ranges	Commercial Courses	**GATOR**
Grades Real Operator Inputs	□ Manual grading	□ Multiple-choice	□ AI-powered doctrinal grading
Adaptive Scenarios	□ Static configs	⚠ Limited paths	□ Living ranges + threat intel
Objective Metrics by Role	⚠ Unit-level only	□ Generic	□ JQR/JCT&CS aligned
Instant Feedback	□ 2-week AAR lag	⚠ End-of-module	□ Real-time chatbot
Predictive Analytics	□ Retroactive	□ None	□ Gap forecasting + prescriptions
Commander Dashboard	□ Excel exports	□ Student certs	□ Role/mission readiness view
Rapid Authoring	□ Weeks per scenario	⚠ Vendor-dependent	□ Hours with templates

Key Insight: GATOR is the **only** solution that grades free-form operator work with doctrinal objectivity and ties it directly to mission readiness.

Credibility & Alignment

□ Mission Match

Built for CMF Workflows:

- Staffed by DoD-experienced technologists
- Deep integration with JQR/JCT&CS cycles
- Tested with operational units

Technology Readiness:

- **TRL-5:** Validated in relevant environment
- Moving toward **TRL-6** via pilots/UAT
- Production-ready architecture

□ Policy Fit

DoD Priorities:

- □ Standardization of training/cert
- □ Improved measurement frameworks
- □ Cyber workforce resilience
- □ Data-driven readiness reporting

Alignment: GATOR operationalizes DoD CIO guidance on cyber workforce strategy at the tactical edge.

> **"We need better ways to measure cyber readiness—GATOR provides the tooling to make that real."**
> — Aligned with DoD CIO Cyber Workforce Framework Strategy

Source: DoD CIO Cyber Workforce Strategy IP Factsheet (FY24)

Metrics You Can Put on a Slide

GAO Finding

DoD has not historically measured or reported domain-level readiness (incl. cyber) in a way that supports commander truth data.

GAO recommends establishing such metrics.

Standards Volatility

JQR/JCT&CS undergo regular update cycles; Services are notified—meaning checklists drift and local binders age fast.

USCYBERCOM J7 annual review process

⚖ Subjectivity Risk

HHQ ESAP exists to ensure *objective* assessments—because unit-level variance is real.

Air Force Stan/Eval policy (ACCI17-202v2)

Training Realism Gap

USCYBERCOM publicly states the need for **more complex** and realistic actors in PCTE scenarios.

Validation that current realism must keep increasing

Sources: GAO-23-106673 | USCYBERCOM GitLab | e-Publishing | DefenseScoop | PEO STRI

Pilot Plan: 60–90 Days

Scope

- **Roles:** 2–3 (e.g., DCO–ID, analytic, hunt)
- **Operators:** 15–30 per role
- **Scenarios:** 5–10 threat-informed exercises
- **Duration:** 60–90 days end-to-end

Measures of Effectiveness

- Rubric agreement rate **≥90%**
- Inter-rater variance **↓50%**
- Authoring time **↓60%**
- Time-to-requal **↓30%**
- Commander dashboard adoption **≥80%**

Deliverables

1. **Baseline Report:** Current readiness snapshot
2. **Post-Pilot Report:** Readiness delta + metrics
3. **AAR Package:** Lessons learned + operator feedback
4. **Data Export:** Integration with JCC2-R or unit systems
5. **Rubric Library:** Co-authored with J7/Stan-Eval

> **Success Criteria:** Commanders can answer "Are we ready?" with quantitative evidence instead of gut feel.

Call to Action

"Let's move from range time to readiness proof."

Next Steps

1. Approve GATOR **enclave pilot** alongside PCTE rotations
2. Co-author rubrics with J7/Stan-Eval
3. Designate pilot unit (15–30 operators)
4. Push results into JCC2-R or unit systems

Contact

Ready to discuss?

Let's schedule a deep-dive demo and discuss enclave deployment requirements.

[Insert contact information]

GATOR: From "we trained" to "we're mission-ready"—with evidence.