True CyberChampion

AI governance, cybersecurity engineering, compliance and AI workforce training for government and commercial organizations

CAPABILITY STATEMENT

truecyberchampion.com

Washington, DC metro area

UEI UEQDZSKKRFGC65 **CAGE** 9DE87 **SAM.gov** Active **Size** Small business

Payment Government purchase card accepted (up to the micro-purchase threshold), or invoice/purchase order for larger engagements

Secure the systems. Govern the AI. Skill the people.

One partner for AI and cybersecurity: engineers who build and harden, assessors who prove compliance, and educators who make it stick.

WHO WE ARE

True CyberChampion is an AI and cybersecurity firm. We govern and secure AI, engineer and harden cloud environments, build the compliance programs regulators expect, monitor security posture continuously, and train the workforce to use AI with judgment, delivered by practitioners who work in federal and regulated environments every day.

CORE CAPABILITIES

Artificial intelligence

NIST AI RMF · ISO/IEC 42001 · OMB M-25-21

AI governance	AI strategy, policy and acceptable use, AI council and Chief AI Officer support, use-case intake and inventory
AI risk	Use-case risk tiering and privacy review (GUAF), AI threat modeling, red-teaming and TEVV, vendor AI risk
Responsible AI	Fairness and bias testing, transparency, human oversight, algorithmic auditing
AI solutions	Rapid prototypes, LLM and RAG systems, governed AI agents, Microsoft 365 Copilot readiness; cloud, air-gapped and classified

Cybersecurity and information security

NIST SP 800-53 · 800-171 · CSF 2.0

Security engineering	Secure Azure landing zones, hardening to MCSB, CIS, DISA STIG and CISA SCuBA, Entra ID and Zero Trust, Defender XDR, Purview, Sentinel, GCC High
Compliance	FISMA, RMF and ATO packages, FedRAMP, CMMC Level 1 and 2, HIPAA, PCI DSS v4.0.1, GLBA, FFIEC and NYDFS
Continuous monitoring	Control monitoring, automated evidence, FISMA and FedRAMP ConMon, executive dashboards and reports
Cyber risk	Risk assessment, virtual CISO and ISSO, third-party risk, business impact analysis, incident response tabletops
Emerging threats	Deepfake fraud, attacks on AI, identity attacks, ransomware resilience, post-quantum readiness

AI workforce training. Customized, role-based AI training built on your own policy, tools and roles, for executives, audit and OIG, legal, finance, data, IT and cybersecurity and every other role. Delivered with our Capability Proof System™, page 2.

Your policy · Your workforce · Your risks · Your scenarios · **Customized training**

COMPANY DATA

NAICS	611430 · 611420 · 541611 · 541690 · 541715 · 541511 · 541512 · 541519 · 518210
PSC	AC12 · AC13 · AJ12 · DA01 · DJ01 · B544 · R408 · R425
ENGAGE	Federal, state and local, commercial, SBIR/STTR, non-profit research · DBA DrBeza.ai

Cloud / hybrid · Air-gapped · Classified · Customer SCIF/SAPF

PAST PERFORMANCE

PBGC — FEDERAL AGENCY

Developed the AI enablement strategy for the Pension Benefit Guaranty Corporation. Supporting the Enterprise Cybersecurity Department's responsible AI adoption through role-based training and AI use cases that improve the accuracy and consistency of work products while saving time and cost.

Cyber — FEDERAL AND DIB

FISMA assessment and authorization support for financial-services platforms, an RMF authorization package for a cleared contractor's classified system, CMMC Level 2 readiness for defense manufacturers, and FedRAMP 20x control mapping.

ISACA — TRAINING PROVIDER

As an ISACA training provider, trained auditors, executives, managers, IT leaders and many other roles, from organizations across sectors, on AI governance, risk and compliance.

Industry — CONTRIBUTIONS

BELGIC Framework (AI skills), DRILL Method (AI skills delivery), iCRAFT Prompts (AI prompting platform) and GUAF (GenAI use-case privacy and risk assessment).

WHAT SETS US APART

- **Practitioners, not presenters.** We build, harden and assess real systems in federal and regulated environments.
- **One program, many frameworks.** Controls built once and mapped to FISMA, CMMC, HIPAA, PCI DSS and GLBA.
- **Evidence included.** Every deliverable comes with the proof an assessor, examiner or auditor will ask for.
- **AI and security together.** We govern AI with the same rigor we apply to security controls.
- **Skills you can see.** People practice on real tasks; we measure what they can do, not who attended.

CREDENTIALS

- D.Eng., Cyber Analytics and AI (The George Washington University)
- M.Eng., Policy and Compliance
- CISSP, CISM, CDPSE, ACCISO
- 20 years in federal government, big tech and consulting
- Key engineering personnel: TS/SCI with CI polygraph (active)

POINT OF CONTACT

Dr. Beza Lefebo

VP, AI Strategy and Workforce Development

240-476-3268 | beza@truecyberchampion.com

11393 Columbia Pike #D10, Silver Spring, MD 20904

From Awareness to Evidence

The Capability Proof System™ for designing, developing, delivering and proving role-based AI skills training

truecyberchampion.com

THE PROBLEM

The awareness trap: why most AI training does not change work

Most AI training is awareness training: a presentation on what generative AI is, a tour of a tool, a slide of rules and a completion certificate. People leave informed, often enthusiastic. Then they return to their desks and little changes. They still do not know which of their tasks AI handles well, which it handles badly, what data they may put in, or how to check what comes back.

The organization has a completion rate.
It does not have a capability.

WHAT CHANGED

The new problem generative and agentic AI adds

Earlier workplace technologies behaved consistently: a spreadsheet adds correctly or it does not. Generative AI does not. The same tool that speeds up one task can quietly degrade another, and who benefits depends on the person and the task.

IMPLICATION

Train by task, which means by role

If AI's usefulness varies by task, then AI training must be organized by task, which means by role. A one-size program cannot tell a budget analyst, a program manager and an auditor where the line falls in their own work. That is the gap the Capability Proof System is built to close.

Awareness is not futile; people need a shared vocabulary and the rules. The problem is that awareness is sold and bought as if it were capability. Leaders approve a program, staff complete it, and everyone assumes the risk is managed and the productivity is on the way. Neither follows.

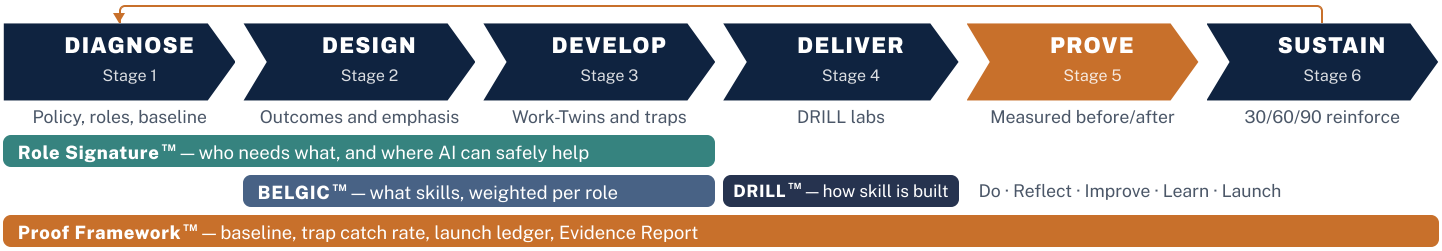
We see seven recurring failure modes. Each one has a known cause in the research, and each one maps to a specific design choice in our system.

FAILURE MODE	WHAT IT LOOKS LIKE	WHY IT FAILS	WHAT WE DO INSTEAD – OUR SYSTEM
1 **Generic content**	One deck for everyone	Transfer depends on how closely training resembles the job	Work-Twin™ scenarios built from each role's real tasks
2 **Passive format**	Lecture, video, demo	Active learning outperforms lecture	DRILL™: learners produce first, then critique and improve
3 **Rules without practice**	A slide of "do's and don'ts" from the AI policy	People can recite a rule and still misapply it in a gray-zone case	Policy-to-Practice drills: sort real cases into Go, Sanitize or Stop
4 **No verification skill**	"Always check the output"	AI quality is uneven	Trap tasks with planted errors
5 **Tool tour, not judgment**	Feature walkthroughs of one product	Features change monthly	Tool-agnostic technique plus your approved tools
6 **One-and-done**	A single session, then nothing	Unpracticed skills fade	30/60/90-day micro-drills and launch check-ins
7 **Measured by satisfaction**	Completion rates and smile sheets	Reaction scores say little about behavior or results	Proof Framework™: work-sample deltas, catch rates, launch ledger

OUR ANSWER

Evidence from each cohort informs the next

The Capability Proof System™: six stages, four integrated frameworks



Every stage ends in a quality gate that must pass before the next begins, and success is defined up front in a signed Outcome Contract.

Four Integrated Framework Components

FRAMEWORK	THE QUESTION IT ANSWERS
Role Signature™	Who needs what, and where can AI safely help in this role?
BELGIC™	Which AI capabilities matter most for this role?
DRILL™	How does a capability become a habit inside a session?
Proof Framework™	Did it work, for whom, and how do we know?

These four components work together as one integrated training framework. Role Signature identifies what matters for each role. BELGIC determines which capabilities to develop. DRILL provides the practical method for building those capabilities through repeated practice. The Proof Framework measures what learners can actually do and whether the training produced meaningful results.

Evidence from each training cohort informs the next, allowing us to continuously refine the curriculum, improve delivery, and strengthen learning outcomes.

OUR PROMISE

Every participant leaves with

1. **A launched work product**
   A real memo, summary, analysis or draft, finished with AI under your rules.
2. **A personal Role Playbook**
   The prompts, checks and principles they wrote themselves.
3. **A measured before-and-after**
   Their own score on time, quality and safety on a task from their job.

Built on research in training transfer, active learning, spaced practice and human–AI work; measured with the Kirkpatrick model and the Success Case Method. We treat participants as professionals adding a tool to an existing craft, not as novices, and in every lab our facilitators narrate how they judge an output, not only what they conclude.

Dr. Beza Lefebo | 240-476-3268 | beza@truecyberchampion.com