CyberFoundry is a cybersecurity and compliance advisory firm specializing in the U.S. Defense Industrial Base (DIB), supporting the design, implementation, and sustainment of security programs aligned with DoD and federal regulatory requirements, including CMMC, NIST, and secure AI adoption.

Subcontractor Role Alignment

CyberFoundry supports prime contractors as a specialized subcontractor providing CMMC readiness, NIST compliance advisory, security architecture, and executive-level cybersecurity leadership in support of DoD programs and task orders.

Core Capabilities

- CMMC Advisory & Readiness (Levels 1–3)
- Gap assessments, scoping, and remediation planning
- Policy and procedure development aligned to NIST SP 800-171/172
- Pre-assessment readiness and evidence preparation
- Executive and board-level briefings
- NIST & Federal Compliance
- NIST SP 800-171 / 172 implementation and sustainment
- DFARS 252.204-7012/7019/7020/7021 alignment
- POA&M development and risk-based prioritization
- Continuous monitoring program design
- AI Governance & Secure Adoption
- NIST AI RMF alignment for AI consumers and integrators
- Shared Responsibility Model (SRM) analysis for AI suppliers
- AI risk governance, policy, and oversight frameworks
- Secure integration of AI into regulated environments
- Virtual CISO / Executive Advisory
- Fractional CISO services for growth-stage and regulated firms
- Security program architecture and operating model design
- M&A security diligence and post-acquisition integration
- Board and investor communications

Labor Categories / Roles Selection

- Virtual / Interim CISO
- CMMC Readiness Consultant
- NIST Compliance Analyst
- Cybersecurity Program Lead
- AI Governance Advisor

CyberFoundry, Inc.

Primary Office:
4015 S. Main Street
#10088
South Bend, IN 46680

New England Office:
396 Roosevelt Ave #6
Central Falls, RI 02863

Principal POC:
Bill Weber, Founder
+1 571 833 3000 (main)
bill@cyberfoundry.io

Web Domains:
https://cyberfoundry.io
https://cmmcbrain.com

Identification Numbers:
EIN: 88-2474514
DUNS: 14-489-5373
(retained for private sect)
SAM/UEI: Pending
(INC-GSAFSD20598142)

Business Properties:
Business Size: 1-50 Emp
NAICS:
(Primary)
541512 Comp Sys Design
(Secondary)
541511 Cust Comp Prog
541519 Other Comp
541690 Tech Consult

Personal DoD Clearances:
DoD Top Secret SSBI
DHS EOD

Differentiators

- Practitioner-Led Delivery
  Led by senior cybersecurity executives and certified CMMC practitioners with decades of hands-on experience.
- Assessment-Ready Focus
  We design programs with the assessor's perspective in mind—clear evidence, traceability, and defensibility.
- Structured Knowledge Systems
  CyberFoundry develops and uses internal knowledge frameworks (e.g., CMMC Brain) to ensure consistency, repeatability, and audit-quality outputs.
- Vendor-Neutral & Outcome-Oriented
  We focus on control effectiveness and risk reduction, not tool resale.

Typical Clients

- Defense Industrial Base (SMBs to mid-market primes)
- Private equity–backed technology and manufacturing firms
- Engineering, R&D, and advanced manufacturing organizations
- Companies preparing for DoD contracts or post-acquisition compliance uplift

Engagement Models

- CMMC Readiness & Pre-Assessment Engagements
- Fractional / Interim CISO
- Compliance Program Build-Outs
- Advisory Retainers

Company Information

- Company Name: CyberFoundry, Inc.
- Focus: DIB cybersecurity, CMMC, NIST, AI governance
- Delivery Model: Advisory, program design, readiness coaching
- Geography: United States (remote-first, on-site as required)

CyberFoundry is available to support teaming agreements with prime contractors and strategic partners across DoD pursuits. The firm provides experienced leadership in capture support, proposal development, and oral presentation preparation, contributing technical content, compliance strategy, and security architecture aligned to federal acquisition requirements. CyberFoundry integrates seamlessly into pursuit teams, supporting primes in developing clear, defensible, and evaluation-ready responses for complex government solicitations.

Principal Qualifications

William (Bill) Roy Muller Weber

Bill Weber is a senior cybersecurity and technology executive with deep experience supporting large-scale U.S. Department of Defense pursuits and programs. Over more than a decade with EDS and Hewlett-Packard Enterprise (HPE), Bill served as a named or key principal on numerous major DoD capture efforts, participating as a core member of pursuit teams responsible for solution architecture, security strategy, and proposal development.

During his tenure at EDS/HPE, Bill played a significant role in developing and delivering RFP responses for complex, high-value federal programs, regularly contributing to written proposals, technical volumes, and oral presentations. His experience includes work on the Navy Marine Corps Intranet (NMCI), serving as a key technical and security resource on the DoD Continuous Diagnostics and Mitigation (CDM) program—a multi-billion-dollar ($6B) cybersecurity initiative—and supporting the design and authorization of HPE's first FedRAMP-authorized Infrastructure-as-a-Service (IaaS) offering.

Bill's background also includes work with MIT Lincoln Laboratory, a federally funded research and development center (FFRDC), where he supported mission-critical government and defense initiatives requiring advanced technical rigor and close coordination with federal stakeholders. Across his career, he has acted as a pursuit lead or senior technical authority for numerous organizations, helping shape winning strategies, articulate defensible security solutions, and instill confidence with government evaluators.

Bill brings to pursuit teams a rare combination of hands-on technical depth, executive-level communication skills, and firsthand experience operating at the scale, complexity, and scrutiny of major DoD acquisitions. He is frequently positioned as key personnel where credibility, security leadership, and delivery confidence are decisive factors.

Resume (https://www.billweber.io/resume/)
Certifications

- Masters in Business Administration (MBA), University of Texas Dallas
- Masters in Science, Information Technology specializing in Security, Capella University
- Bachelor of Science, Computer Information Systems, Excelsior College
- Certified CMMC Assessor (CCA)
- Certified CMMC Practitioner (CCP) CPN 62743
- Registered Practitioner Advanced (RPA)
- Registered Practitioner (RP)
- (ISC)^2 CISSP 29867
- ISACA CISM 1014442 / CRISC (1004569) Expired
- OneTrust Fellow of Privacy Technology 73644
- Microsoft Certified System Engineer (MCSE / MCITP) 1793697
- Amazon Web Services Certified Cloud Practitioner (CCP) 01783372
- Cisco CCNA/CCDA CSCO010095762
- NSA IS Security Pro / System Admin / InfoSec Assessment Method (CNSS 4011/4013)
- ICCP Certified Computing Professional (CCP) 240331
- CompTIA A+ / i-Net+ / Server+ / Network+ / Cert Tech Trainer (CTT+) COMP10445345