COALFIRE FEDERAL

Cyber program management and operations

Coalfire's comprehensive program management led by industry experts augments your organizational staff's capabilities. Our team helps orchestrate people, processes, and technology to detect, respond, and manage security incidents. Outsourced cyber subject matter expertise fulfill management and operational mission objectives.

Legacy methods to thwart cyber threats are no longer effective due to the rapid pace at which new vulnerabilities emerge and threats evolve. Get true security through a programmatic approach that unifies point-in-time assessments with continuous diagnostics and mitigation (CDM). Dramatically increase the effectiveness of your organization's information security risk management program by:

- Implementing new risk management methods, such as the Department of Homeland Security's (DHS) CDM and the National Institute of Standards and Technology's Information Security Continuous Monitoring (ISCM) to develop, mature, and maintain a robust security program
- Combining traditional program management with project governance (including policy, organizational structure, engineering lifecycle management, outreach, and training) to build a more effective, large-scale security program
- Assessing your program's baseline capabilities using risk scoring, data analytics, and visualization

Why Coalfire

- Certifications to meet a multitude of contractual requirements.
- A deep understanding of the nuances of government IT at the federal, state, and local levels.
- Over a decade of experience providing a full range of long-term and short-term cybersecurity solutions to government clients, including:
  - Guidance on Department of Defense (DoD) Risk Management Framework
  - Interpretation of NIST for application to government requirements
  - Skilled staffing to meet your mission-critical cyber project needs
  - Mobile application security assessments
  - Designing and implementation of large-scale CDM programs
  - Security architecture creation
  - Implementation of programs with custom training support

CERTIFIED TECHNICAL EXPERTS IN LEADING CLOUD, ENCRYPTION, VIRTUALIZATION, AND CONTINUOUS MONITORING SOLUTIONS

DoD client focus: The largest DoD service provider

The essential services provider for the entire DoD, our client provides the full range of IT equipment, services, solutions, and customer support to help numerous offices meet mission and business requirements. As their information assurance (IA) needs grew, our client awarded us a five-year contract because of our extensive experience with IA services. Our team quickly established IA solutions to support a full spectrum of engineering, risk management, assessment, and compliance activities for the IA enterprise.

Upon contract initiation, our program management approach allowed us to coordinate a smooth transition, minimizing government resources and intervention, with little to no degradation or interruption in service. We completed an aggressive 15-day transition to phase-in a large team of 36 cybersecurity professionals, and we continue to maintain full staffing via an intensive recruiting and screening process that allows quick certification and acceptance at the client organization. Supported by our team's thorough implementation of automation and process efficiencies, our client has experienced 100% growth in their customer mission (an increase from 7,500 users to more than 20,000; approximately 125 accredited systems to more than 225; and 15,000 assets to nearly 50,000). We have also saved the government nearly $6M per year, while increasing our own level of support by 20% (36 to 43 full-time employees).

Using a phased approach over the course of three months, we transitioned our client from the Retina vulnerability management solution to the Assured Compliance Assessment Solution (ACAS), ensuring no interruption to risk and compliance management requirements while introducing technical and process efficiencies. Along with the introduction of ACAS, our team has implemented new processes (for example, a "Top 10 Vulnerable Systems" weekly hit list, System administrator-focused Iraq and Afghanistan Veterans of America [IAVA] and Security Technical Implementation Guide [STIG] training, and an internally focused command cyber readiness inspection [CCRI] effort). These processes have reduced system vulnerabilities by more than 95%.

TRUSTED INSIGHT FOR NAVIGATING THIS COMPLEX CYBER WORLD

GSA Schedule 70

- 132-45A Pen Test
- 132-45C Cyber Hunt
- 132-45D Risk & Vulnerability Assessment (RVA)

Other contract vehicles

- CDM BPA Subcontractor
- SeaPort Enhanced prime contract

GSA IT Schedule 70 Contract Holder

SeaPort-e

CMMI Services Maturity Level 3 | Accredited FedRAMP 3PAO, PCI QSA and HITRUST CSF Assessor | Certified ISO 9001 (2015), ISO 27001 (2013)
CONUS/OCONUS Support Capability | System for Award Management Registered

CAGE Code: 36BY6 | **DUNS #:** 184456155 | **NAICS:** 541519, 541512, 541513, 541611, 541690, 541511

COALFIRE FEDERAL

Cybersecurity that fuels success | CoalfireFederal.com | 877.224.8077