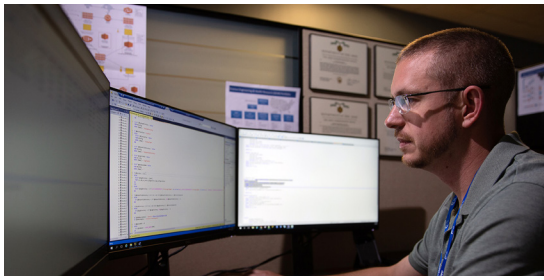
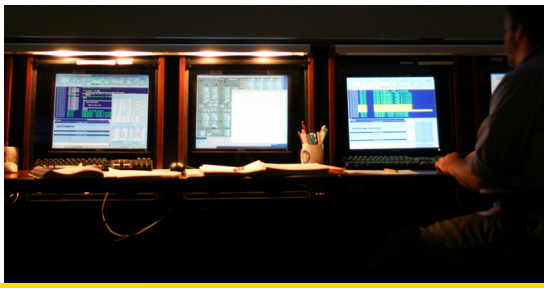
Cybersecurity

Implementation and Operations





KBR CAPABILITIES

KBR 's integrated security approach enhances security posture, protects data and operations, and mitigates security vulnerabilities in dynamic threat environments, while respecting cost and schedule constraints. Our information security-certified cybersecurity technical staff of approximately 200-plus people, along with our cutting edge cyber labs and proven system engineering processes, ensure security is designed into every product and meets all customer needs.

KBR ADVANTAGES

- A trusted government partner providing innovative, technology-focused solutions
- Highly technical, experienced, and mature employee base focused on customer mission; more than 15,000 professional and technical staff with all levels of security access
- Core competencies in scientific data processing and visualization, mission critical operations and control systems, agile software development, predictive and diagnostics analytics, and intelligent and autonomous systems

KBR OFFERINGS

Cybersecurity Solutions

- Maintain leading edge cyber labs and cyber range
- Perform computer network defense
- Provide cybersecurity engineering and operations
- Implement Risk Management Framework (RMF)
- Accredit systems and obtain Authority to Operate (ATO)
- Develop secure software and systems using DevSecOps processes
- Perform Independent Verification and Validation (IV&V)
- Provide cybersecurity training

Critical Infrastructure Protection

- Implement Industrial Control Systems (ICS)
- Support Supervisory Control and Data Acquisition (SCADA)
- Perform Vulnerability and Mitigation Assessments
- Provide secure solutions for cyber-hostile environments
- Install large scale and complex systems
- Design and implement software and program control systems
- Integrate advanced software technology
- Provide and operate a cyber range with information and operational technology profiles

KBR OFFERINGS CONT.

Electronic Security

- Physical access control system
- Surveillance
- Perimeter and intrusion detection
- Mass notification systems
- Closed circuit television
- Install and sustain security systems
- Force protection assessments
- Design and develop operational centers

Cybersecurity Incident Responses

- Develop/validate Incident Response Plans
- Support cyber exercises and remediate incidents
- Perform forensic investigation and develop tools

INFORMATION TECHNOLOGY

IT Solutions for Mission-Focused Programs

- Enterprise computing services
- Application services
- Cybersecurity solutions
- Modernization and cloud transitions
- Data analytics and data implementation
- Network sustainment and modernization

KBR CERTIFICATIONS

- AS9100:2016
- ISO 9001:2015
- ISO20000-1:2011
- DCMA approved purchasing system
- DCAA approved accounting system

aws partner network

Select Consulting Partner

Public Sector Partner

DEMONSTRATED SUCCESSES

Federal Aviation Administration (FAA)
Information Security Architecture and Information System Security Assessment support for Enterprise Network Services and aviation information access program.

National Highway Traffic Safety Administration (NHTSA)
Cybersecurity Incident Response Plan support, Security Assessment and Authorization support for large-scale data repository and analysis system.

Department of Transportation (DOT)/Department of Homeland Security (DHS)
Established and developed cybersecurity project portfolio supporting technology-oriented public-private partnership. Development of plans, Risk Assessment, Best Practices reports.

Federal Motor Carrier Safety Administration (FMCSA)
Established cloud-based test environment for FMCSA application development, supported technical architecture to meet federal regulation compliance, custom web-based security training.

Major Automotive Manufacturer
Researched and developed threat injector using ECM port available on all modern automobiles, developed wireless attack methods using WiFi and Bluetooth, reverse engineered proprietary ECM codes to develop penetration testing strategy.

DoD/U.S. Navy
Led Information Assurance Certification and Accreditation transition to new risk-based framework, cybersecurity tool development, vulnerability assessments.

NASA
Full range of security services support for multiple centers and programs.

NOAA
Support to SOC, SIEM system, and continuous monitoring program.

Department of Interior (DoI)
Support to SOC, SIEM system, and continuous monitoring program.

KBR