Boston Government Services, LLC

At BGS, we are effective with people and efficient with technologies. Our partnerships with key technology providers enable us to deliver innovative solutions to advance cyber research initiatives, solve costly and time consuming problems, and protect our critical infrastructure. Our highly-qualified experts with cutting edge research experience enable us to provide valuable unique resources in a landscape of rapidly evolving threats and new technologies.

Preparing Companies for NIST 800-171 DFARS & DOE Order 205.1C Compliance

Organizations handling government data must be compliant with NIST 800-171 DFARS requirements. BGS assesses organizations for compliance with these requirements, delivers gap analysis, and provides guidance on addressing deficiencies.

Mission-Focused Solutions
www.BGS-LLC.com

SERVICES

CYBER SECURITY

Our Center for Cyber Security Innovation addresses critical infrastructure needs, supports cyber research initiatives, and delivers Cloud SOC capabilities. Our experts perform compliance assessments and deliver fully-compliant solutions in highly-regulated and complex environments.

RESEARCH & CRITICAL INFRASTRUCTURE
- Protect Industrial Control Systems Security (ICS/DCS/SCADA)
- Secure Internet of Things (IoT) & communication devices
- Analyze and address Supply Chain threats
- Perform threat analysis and risk mitigation
- Secure across protection boundaries
- Secure cloud environments
- Address incident response needs
- Create Mission Impact Analysis & Contingency Plan

COMPLIANCE & ASSESSMENTS
- Perform compliance assessments (NIST 800-53; NIST 800-171; CSF Framework, CMMC Preparation, etc.)
- Red/Blue Team capabilities; Scan, Test, and Evaluate (ST&E)
- Policy, Procedure, and Plan Development and Maintenance
- Vulnerability, Threat, and Risk Assessments with remediation
- Incident Response & Reporting
- Certification & Accreditation/Security Authorization Packages for ATOs
- Continuous Monitoring Program Planning and Management
- Secure all classification levels and categories
- Security Awareness and Training

SECURITY OPERATIONS CENTER (SOC)
- Real-time security event monitoring (SIEM) and analysis
- On-premise, Cloud, or Hybrid solution provider
- Detect, triage, and remediate potential incidents
- Data Trending, Metrics, and Reporting
- Malware Reverse Engineering
- Cyber Threat Intelligence from Multiple Threat Intelligence Sources and Threat Hunting
Experience Highlights

- Providing all Cyber Security support services for General Support Systems, Industrial Control Systems, and operational technology for the Department of Energy across multiple sites. Tasks include:
  - C&A package creation and maintenance
  - Risk assessments
  - Privacy program compliance
  - Mission impact assessments
  - Contingency planning
  - Incident response
  - System security plans
  - Device characterization
  - Supply Chain reviews
  - Plan of actions and milestones
  - Security assessment reports
  - Implementation and maintenance of cyber security tools
  - Cyber awareness training
  - Continuous monitoring support

- Creation of certification and accreditation packages for the DOE Office of Environmental Management Los Alamos Legacy Cleanup Contractor for telemetry, portable devices, and enterprise and cloud-based systems.

- Blue Team Assessments for NNSA facilities
- NIST 800-171 assessments for commercial organizations providing support to the U.S. government and military to ensure compliance.
- NIST 800-53 assessments for ICS and General Support Boundaries compliance for DOE facilities.

THE BGS DIFFERENCE

BGS attracts and retains subject matter experts in their field. The BGS Center for Cyber Security Innovation brings expertise from government programs, national laboratories, research institutions, military cyber threat teams, intelligence community professionals, and critical infrastructure to provide customers with innovative services and solutions. BGS assesses, designs, and manages cyber security programs for all types of environments using Security by Design principles. Our highly skilled professionals are well-versed at navigating across information protection zones while ensuring information confidentiality, integrity, and availability at the appropriate level, regardless of classification requirements. The BGS CCSI encompasses core areas of:

- Compliance assessments
- Cyber Security research
- Critical infrastructure support; and
- SOC capabilities

ADDRESSING EMERGING CHALLENGES

BGS focuses on addressing emerging challenges and solving complex problems. Our cyber security expertise in nuclear security, engineering, and research, along with our understanding of operational requirements to meet mission needs sets us apart.

ICS/DCS Challenges: ICS security has become more challenging with targeted attacks against devices once believed to have “Security through Obscurity.” The geographical challenges of distributed control systems add a layer of complexity and increases the threat landscape. Our ICS cyber specialists enable mission needs for customers with a proven Defense-in-Depth approach to isolate critical assets appropriately and secure core components, while enabling secure connectivity to address mission requirements. We monitor ICS systems without impacting the operational integrity or availability of the system.

IoT Challenges: A rapid influx of IoT devices absent of basic security design principles have altered the cyber threat landscape and increased organizational risks. Devices of all kinds have become Internet-enabled to connect people and functions to devices. This interconnected world was developed with low cost methodologies rather than security-minded principles, resulting in organizations deploying devices without security features. BGS assesses IoT security, addresses vulnerabilities, and monitors the environment to ensure the mission is not impacted. We work with emerging technologies to deliver Cyber Security by Design.