Global Solutions Group, Inc. (GSG) is a multi-faceted innovative technology and professional services company incorporated in 2003. GSG is currently prime contractor for Cybersecurity, Digital Transformation, and IT Services and is actively working with multiple federal government agencies including DoD and Civilian agencies, as well as over 75 state and local government agencies, successfully managing over 100 active projects. GSG has collectively completed more than 1000 Cybersecurity projects.

CASE STUDIES

U.S. Department of Agriculture
Multi-year BPA of Cybersecurity Assessment, Web Security Assessment and Penetration Testing

Scope:
- Perform Operational Security Assessments, Penetration Testing and Web Security Assessments for USDA
- Quarterly & Ad Hoc Penetration Testing of the entire USDA’s Systems, network A&I environment
- Web Security Assessments of High Value USDA Applications

Solutions:
- Cybersecurity Assessments and Penetration Testing Services to over 21 sub-agencies of more than 45,000 USDA and users located in more than 3,400 fields across the country
- Cybersecurity Assessment Services to around 15 Data Centers, 105,000 Workstations, 15,000 servers and 100,000 Endpoints
- Scanned 500,000 IP’s on Penetration Testing
- Examining and Evaluating the agency’s Operational Security Policies, Procedures, and Systems
- Identifying strengths, vulnerabilities & agency security posture
- Identifying and evaluating attacker tactics and methods
- Developing / mapping identified threats for agency’s assets
- Developing a master list of threats or “findings”

U.S. Department of the Interior
Information System Security Line of Business (ISSLOB) Support Services

Scope:
- Comprehensive Services that involve performing full-scale System Assessment and Authorization audits or System Assessment Only audits, and Targeted Services that involve performing discrete specific security-related audit functions based on the customer agency’s need.

Solutions:
The following are the responsibilities of GSG to perform on call order basis:
- Risk Management Framework (RMF) Development and Integration
- Assessment and Authorization (A&A) Services
- Continuous Monitoring Strategy Development
- Continuous Monitoring Program Evaluation
- OHS Compliant High Value Asset (HVA) Assessments
- Technical Testing and Penetration Testing
- Forensics + Social Engineering + Insider Threat Assessment
- Security Policy, Plans and Documentation Development and Testing
- Federal Risk and Authorization Management Program (FedRAMP) Documentation Development and Preparation
- Plan of Action and Milestone (POA&M) development
- Various Governance/Risk Compliance (GRC) Tool Support
- Supply Chain Risk Management (SCRM) strategy and assessment
- Federal Risk and Authorization Management Program (FedRAMP) Documentation Development and Preparation
- Various Governance/Risk Compliance (GRC) Tool Support
- Supply Chain Risk Management (SCRM) strategy and assessment
- WiFi assessment
- Identifying strengths, vulnerabilities & agency security posture
- Identifying and evaluating attacker tactics and methods
- Developing / mapping identified threats for agency’s assets
- Developing a master list of threats or “findings”
## Governance
- Strategy Consulting
- Security Program Consulting
- Policy & Procedure Development
- Virtual CISO services
- Business Continuity Planning
- Disaster Recovery Audit
- Operational Continuity Planning
- Security Compliance - NIST, CMMC, HIPAA, PCI DSS, SOC2, PII, CIS, CJIS, FISMA, FEDRAMP, FERPA, ISO, and Control Validation

## Audit & Compliance
- Security Framework Gap Assessments
- Security Audits and Certification Services
- Third-Party Review And Policy Development
- WorkFlow Development
- Cybersecurity Risk Assessments
- Risk Management
- Cloud Security Reviews
- Assessment And Authorization (A&A)
- Third Party Risk
- Data Risk Intelligence
- Information Assurance

## Managed Security Services
- Managed Detection and Response Services
- 24/7/365 Security Operations Center (SOC)
- Security Awareness Services
- Managed IT Security Services
- Managed Threat Detection and Response
- Incident Response Planning
- Incident Response (Retainer with SLA)
- Threat Hunting
- Threat Intelligence
- Digital Forensics
- Continuous Vulnerability Monitoring
- Lateral Movement Detection
- Active Directory Assessments
- Security Information and Event Management (SIEM) Optimization
- Security Validation
- Automated Defense
- Attack Surface Management
- Security Hardware and Software

## SMART Security Surveillance
- Security Camera Design, Installation, and Configuration
- Safety and Security Alerts using Advanced Video Analytics
- Just-In-Time Detection
- Real-time Alerts
- Incident Response Management
- Physical & Electronics Security (Assessment, Integration, Automation)
- Access Management: RFID and License Plate Recognition

## IoT and Automotive Security, ADAS & CVIP
- Advanced Driver Assistance System (ADAS)
- Computer Vision & Image Processing (CVIP)
- Porting and Optimization on Embedded Platform
- Electric and Autonomous Vehicles - TARA Assessment
- ECU Security Assessment (Specific unit and interfaces)
- Car Security Assessment of External Interfaces
- Security Assessment of Adjacent Systems: Automated Parking (Sensors, Geolocation, WPT)
- Car Security Assessment (ECUs Hardware, Software, and Networks)
- Web and Mobile Application Security Assessment
- Penetration Testing

### NIST and CMMC Capability
In order to support customer organizations in complying with the cybersecurity requirements set forth by both NIST and CMMC 2.0, GSG supports in providing the NIST SP 800-171/800-172 and CMMC 2.0 compliance guidance. Additionally, GSG offers insight into the deployment of cyber risk management solutions across the business.

Our experts support your business/organization by:
- Performing gap analysis for NIST & CMMC 2.0 assessment
- CMMC 2.0/NIST framework readiness assessment
- Compliance/Risk assessment maturity status and
- Managed support for CMMC 2.0 framework implementation

Our team will support your organization to meet DoD’s cybersecurity requirements and simplify the process to implement and comply with CMMC 2.0.