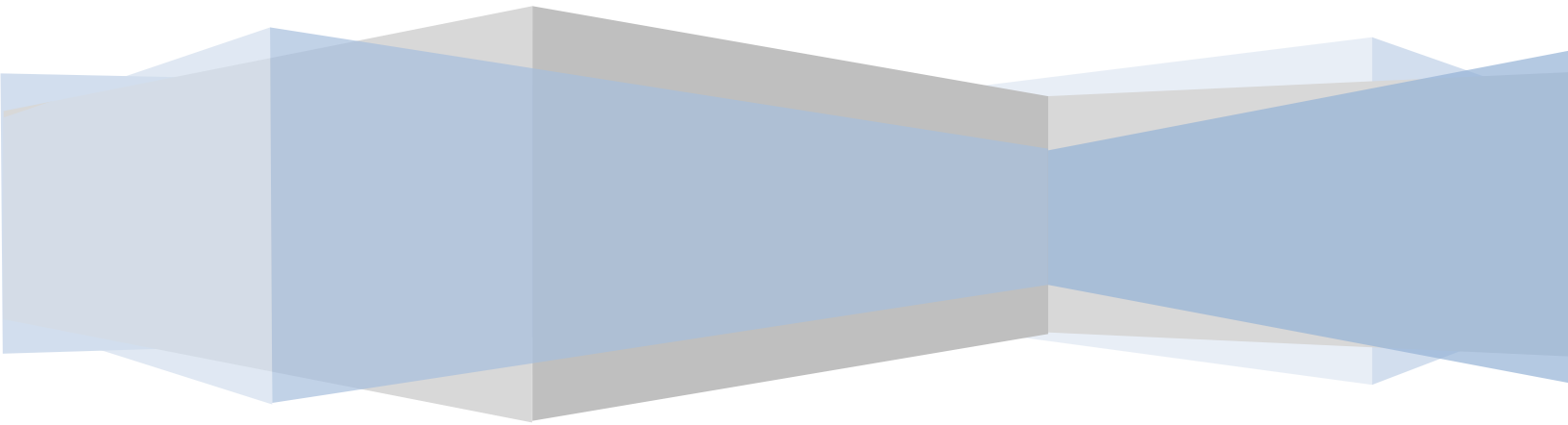
MCGLOBALTECH

BRIDGING THE GAP BETWEEN MISSION, TECHNOLOGY & SECURITY

MCGlobalTech

Cybersecurity Capability Statement



MCGlobalTech 1325 G Street, NW Suite 500 Washington, D.C 20005 | Phone: 202.355.9448 | www.mcglobaltech.com

Table of Contents

About MCGlobalTech

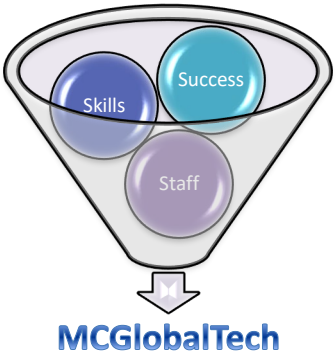
McBorrough Cody LLC dba MCGlobalTech is a 100% Minority-Owned Small Business founded by industry leaders to provide strategic advisory and information security consulting services to public and private sector business leadership. MCGlobalTech's mission is to better align an organization's enterprise technology and security programs with their global vision and business objectives.

MCGlobalTech is a Registered Provider Organization approved by the Cyber Accreditation Body to support the US Defense Industrial Base with cybersecurity advisory and consulting services to develop enterprise cybersecurity programs in compliance with National Institute of Science and Technology (NIST) standards and the Cybersecurity Maturity Model Certification (CMMC).

Our mission is to be a trusted provider of information technology services and solutions with core competencies in cybersecurity, information assurance, security engineering, risk management and security program and project management. Our proven methodologies and scalable solutions help our clients achieve maximum return on their investment.

At MCGlobalTech, we believe that strong values create long-term relationships with our customers, employees, partners and the communities we serve. At the heart of everything we do, our corporate values are:

- Providing customer satisfaction
- Delivering innovative solutions
- Empowering staff for success
- Maintaining technical excellence



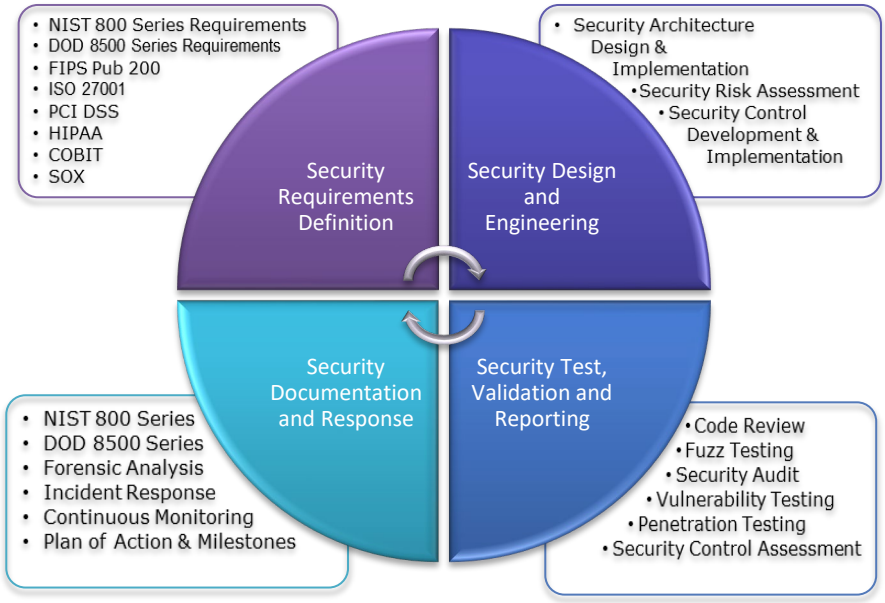
MCGlobalTech consultants provide a number of innovative services and solutions to produce a comprehensive risk based protection strategy to protect our client's data and mission critical systems. By partnering with MCGlobalTech, you can be assured of a tailored security program that fits your unique business requirements instead of a cookie cutter – canned solution. MCGlobalTech also partners with other service providers such as industry-focused corporations, technology vendors and security organizations to enhance and balance our portfolio of services.

The time and cost savings achieved from the MCGlobalTech proven Assess-Plan-Implement-Monitor, (APIM) service delivery methodology allows organizations to spend more energy and resources in addressing their specific risks. Our professionals assist organizations in applying the results of vast industry knowledge base to their unique business requirements so that potential gaps can be identified and addressed accordingly. Security should never exceed the cost of the actual asset you are trying to protect! If your business can benefit from this type of

innovative partnership, add MCGlobalTech to your team of professionals.

Full Life-Cycle Security Support

MCGlobalTech provides full life-cycle information security support to ensure that federal agencies and commercial companies meet their regulatory and business security requirements. Our security life cycle services provide support from system conception to system operation. Our services can be procured as a complete package or individually depending on where you are in your system's life cycle.



Cyber Security Assessments

MCGlobalTech has specialized services and solutions that pertain to security assessments. MCGlobalTech provides a variety of assessment services that include Attack & Penetration, Testing and Validation, Risk Assessments and Vulnerability Assessment/Management. MCGlobalTech has a core team of subject matter experts that perform these services on an exclusive basis to all of our clients. MCGlobalTech has developed detailed methodologies and processes for assessing the following technical areas:

- System Level (workstation and servers)
- Network Level (firewall, routers, switches, IDS, VPN, etc.)
- Applications (web-based)
- Wireless
- Telephony

A top-to-bottom assessment of external and internal access is performed to assess the effectiveness of the organization's current posture in addressing its security risks and exposures.

Security Authorization (Assessment and Authorization)

The primary goal of MCGlobalTech's Security Authorization (SA) Program is to ensure that Federal Agencies are able to meet their customer's needs with a well-defined SA process. Thus, using the 80/20 rule, 80% of the needs of the stakeholders can be addressed in a clear and concise S&A process. Systems enter a repeatable, established and fully documented S&A process, pass through the process using clearly defined procedures and automated scanning and exit consistently. Drawing on our extensive experience, MCGlobalTech can address the remaining 20% of stakeholders needs by providing guidance and recommendations involving management, operational and technical controls and activities.

Accomplishments realized by MCGlobalTech's SA program include the following:

- System Baseline Security Requirements
- Providing Stakeholders the ability to better measure the progress of SA engineering and re-engineering activities
- Identifying and completing critical deliverables over a period of time in a systematic and rational manner
- Obtaining feedback and deliverables acceptance prior to working on additional activities or deliverables
- Ensuring resources are concentrated on completing tasks associated with the current phase, providing focus and advancing progress
- Providing a model that can be published to stakeholders, detailing the organized flow of engineering/reengineering activities being performed in SA Program
- Standardization, consistency, efficacy and efficiency in initiating and completing Assessments and Authorizations

Critical components of MCGlobalTech's SA program process includes:

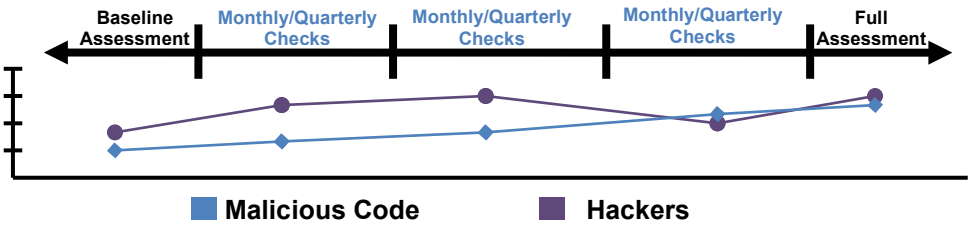
- System Characterization (FIPS 199)
- Security Self-Assessments (NIST SP 800-26)
- Security Risk Assessments (NIST SP 800-30)
- System Security Plans (NIST SP 800-18 and NIST SP 800-53)
- Security Test and Evaluations (NIST SP 800-53)
- Plan of Actions and Milestone (POA&M)

Security Continuous Monitoring

MCGlobalTech's Security Continuous Monitoring (SCM) program is designed to help Federal Agencies and commercial clients meet existing Government regulations including the Federal Information Security Management Act (FISMA), ISO 27000, PCI DSS, HIPAA, SOX and all other federal security requirements or directives. The SCM gives organizations the ability to respond to both internal and external audits and existing and new security threats and vulnerabilities. MCGlobalTech's SCM

program will not only enable proactive responses to Federal information technology security regulatory requirements but will also help organizations improve the management of their security risks.

The MCGlobalTech SCM program is designed to review the security posture of an agency on a recurring basis. The audit and vulnerability scanning will occur on a monthly and/or quarterly basis and will include a full baseline assessment at the beginning of each fiscal year. The program is designed to measure an organization's security posture over time. This will allow management to understand whether the security of the network is improving or declining and determine what areas to focus available resources.



Security Risk Management

MCGlobalTech's Security Risk Management (SRM) Program incorporates processes that describe the procedural steps to identify, capture, escalate, mitigate, and manage business risks and material weaknesses. Our SRM program provides our clients with a means to enhance systems security and operational performance and facilitate informed decision-making. The SRM program is a metrics-based program that measure risks and performance throughout the life cycle in an iterative approach – before, during and after. The SRM process principal goal is to protect the client and its ability to perform its mission, not just its IT assets. Additionally, MCGlobalTech's SRM coordinates the synchronization of potential impairment to operations with effective levels of security controls and mitigations. The SRM allows for managing security risk (to include interdependencies), developing policies, ensuring policy compliance, monitoring the adequacy of the certification and accreditation process, and managing and prioritizing risks identified through a consolidation of *Plans of Action and Milestones* (POA&M's) for effective resource utilization (funding and time sensitivity).

The benefits of MCGlobalTech's SRM include:

- Eliminating material weaknesses
- Streamlining responses to internal and external data calls (GAO, IG, ad hoc reports)
- Effectively address risks and risk drivers across the enterprise
- Establishing a basis for prioritization of an effective resource utilization
- Facilitating accountability through assignment, management and tracking risk mitigation activities
- Establishing a centralized repository of reusable data

- Facilitating and monitoring policy implementation and effectiveness
- Supporting security decision-making through establishment of an integrated security readiness/preparedness dashboard

Security Engineering

Infusing security principles and disciplines into the business continuum is critical to accomplishing the mission of private sector entities and government agencies. Implementing inter-reliant security assurance engineering within the current production is a proven method for affecting progressive change within client organizations. Most organizations are continually seeking government and industry practices to improve their business operations. Security assurance engineering leverages applicable agency and industry practices that prescribe methodologies to improve and ensure the business continuum.

To address the vast and continually changing technology landscape, MCGlobalTech employs specific industry-proven technology practices. MCGlobalTech's security assurance engineering process utilizes security technology best practices, security systems integration and lessons learned, to provide proven security guidance to system and application developers. Above all, MCGlobalTech's security assurance engineering program focuses on and is driven by business and mission requirements. Requirements provide the guidance of what to do (how to apply the practices and standards) and facilitate synchronization of the security requirements and functional business requirements enabling the client's mission.

MCGlobalTech's assurance engineering program consists of:

- Security Requirements Definition
- Security Requirements Implementation
- Security Requirements Testing and Validation
- Security Requirements Documentation and Monitoring

Security Architecture Services

Security Architecture Services addresses systemic causes of vulnerabilities to ensure that the cost of system failure, recovery, business interruption, and reputation impact is diminished. Our enterprise-level, top down approach considers business, operational and IT strategies to design security solutions. MCGlobalTech implements a six phased approach to develop a security architecture design that is spread across data, application and infrastructure architectures to achieve compliance with legislation and industry regulations. .

- Develop Security Policy Definition
- Identify System Security Requirements
- Develop Technical Security Specifications
- Design the System Security Architecture
- Implementation of Target Security Architecture
- Implementation of Security Practices to Maintain Secure State

Network Security

Network Security Services addresses management and control of enterprise technology through implementation of leading edge security administration, remote access, network security monitoring and access control solutions. MCGlobalTech's technology integration solutions are designed to facilitate the implementation of mission critical solutions. Thus, we consider each of our integration solutions to be critical success elements that reflect the core technological competencies required solution. These elements include:

- Firewall/router Solutions
- Intrusion Detection/Prevention Solutions
- Virtual Private Network Solutions
- Remote Access Solutions
- Anti-Virus solutions
- Encryption Solutions

MCGlobalTech's Management Experience

MCGlobalTech's leadership team is comprised of subject matter experts that have performed in senior management positions within some of the most respected organizations in both government and commercial industry. One of MCGlobalTech's critical success factors is leveraging this knowledge across all of our clients. The following is a sample of organizations that have contributed to the backgrounds of our leadership organization:

Federal Clients

Clients	Information Assurance	Vulnerability Management	Security Risk Management	Security Engineering	Penetration Testing	Network Security
DHS	•	•	•	•	•	•
DOL	•	•	•			•
IRS	•	•		•	•	
NASA	•	•	•			
DOT	•	•	•			
DOD	•	•	•	•		•
FBI	•		•			
VA	•	•				
USAID	•	•				•

Commercial Clients

Clients	Security Program Management	Security Risk Management	Security Engineering	Penetration Testing	Vulnerability Management
FISERV	•	•		•	•
Verisign	•	•			
CarMax			•		•
Freddie Mac		•			
Booz Allen	•	•	•	•	•
Hawaiian Healthcare	•	•			
Bancroft	•	•			
Lydall	•	•			
EJC Systems	•		•		
Walgreens	•		•		

Certifications

MCGlobalTech professionals maintain a number of professional and technical certifications to include:

- Certified Information Systems Auditor (**CISA**)
- Certified Information Systems Security Professional (**CISSP**)
- Certified Information Security Manager (**CISM**)
- Certified Ethical Hacker (**CEH**)
- Certified in Risk and Information Systems Control (**CRISC**)
- Certificate of Cloud Security Knowledge (**CCSK**)
- Certified Business Continuity Professional (**CBCP**)
- CheckPoint Certified Systems Engineer (**CCSE**)
- Information Technology Infrastructure Library (**ITIL v3**)
- Program Management Professional (**PMP**)

Corporate Designations

- Minority Owned Small Business
- Self-Certified Small Disadvantage Business
- Cage Code: 76X97
- DUNS #: 967264701

NAICS Codes

518210, 541512, 541513, 541519

Technology Partners

Microsoft, IBM, SentinelOne, Proofpoint, Datto, Duo, Bitdefender, Webroot, Veeam, Axcient, Cymulate, NeQter Labs, Preveil, Perimeter 81, Infrascale, BitTitan, Ironscales, Acronis, Dropsuite, and Ninjio

Contact Information

MCGlobalTech
1325 G Street, NW
Suite 500
Washington, D.C 20005
Phone: 202.355.9448
Email: info@mcglobaltech.com
www.mcglobaltech.com