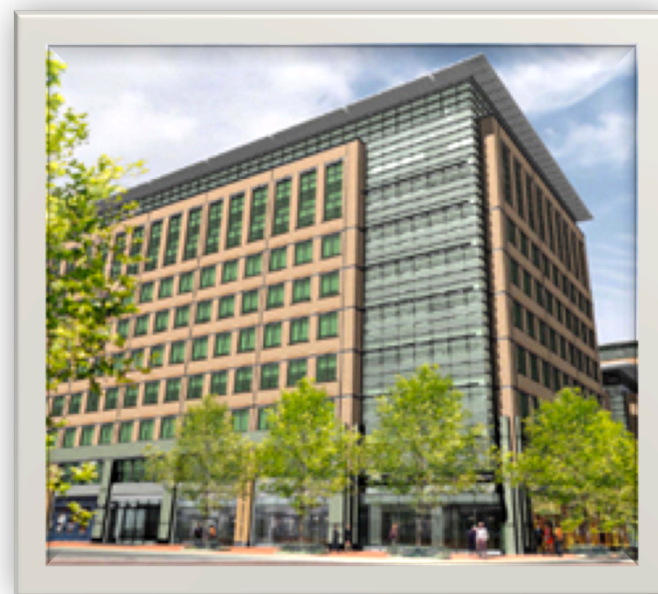# EmeSec Incorporated Corporate Capabilities

ENSURE::MANAGE::EVOLVE::SECURITY

EmeSec: Exclusive Focus on Information Assurance and Cyber Security

- Founded in 2003

- Headquartered in Reston, VA

- $7M size standard

- Top Secret facility clearance

- ISO 9001:2008, ISO/IEC 20000-1:2005, and ISO/IEC 27001:2005 certifications

EmeSec is a certified SBA 8(a) and GSA certified woman-owned (WO) small disadvantaged business, as well as a Service Disabled Veteran Owned Small Business (SDVOSB)

EmeSec is a Quality Organization Focused on Reliable Performance and Customer Satisfaction
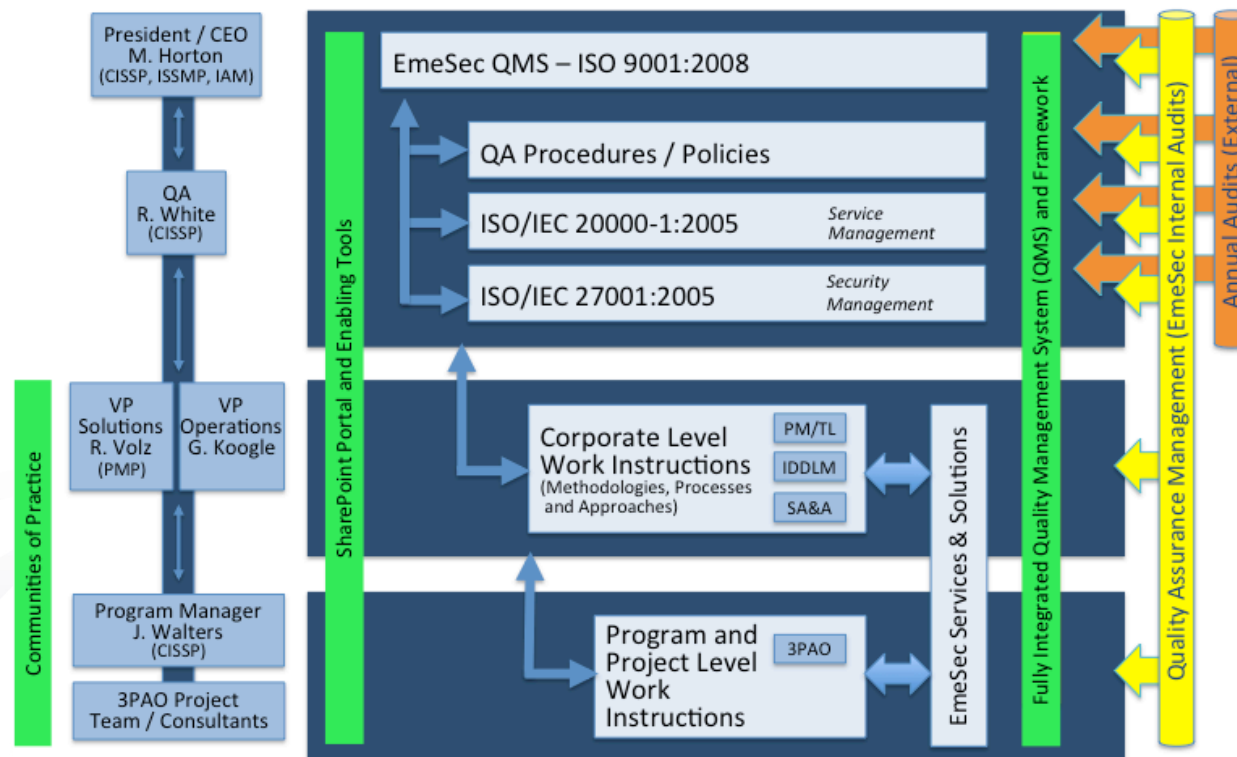
EmeSec has the qualifications and certifications of a large company with the agility and responsiveness of a small one

BD-TM-005

Recognized thought leadership applied towards solving information assurance challenges posed by cyber threats, cloud computing, mobility, and information lifecycle management

- Active leadership in Industry Advisory Council (IAC), AFCEA

- Co-authorship and active member of NIST cloud technology working groups

- Curriculum Advisor for local DHS CyberWATCH program

- Sought-after panelists and speakers

BD-TM-005

Experts who are perceptive, bold, resourceful, and committed …. and highly skilled and certified

WE ARE EXPERTS...
Experienced, knowledgeable and credentialed in everything security

WE ARE PERCEPTIVE...
Strategic, acute, clearheaded, quick, clever approach to solving problems

WE ARE BOLD...
Fearless, spirited, straightforward, fresh, unconventional thinking to tackle evolving threats

WE ARE RESOURCEFUL...
Nimble, delivering custom, maximum value solutions

WE ARE COMMITTED...
Stalwart, results-focused, united in service with the customer to the mission

90% of EmeSec Technical Staff Possess Multiple Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Certificate of Cloud Security Knowledge (CCSK)
- Information Systems Security Mgmt. Professional (ISSMP)
- NSA InfoSec Assessment Methodology (IAM)
- Comp TIA Security+, A+, & Network +
- Certified Authorized Professional (CAP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Entry Networking Technician (CCENT)
- Red Hat Certified Technician (RHCT)
- VA-Cyber Security Practitioner (VA-CSP)
- Federal IT Security Professional-Auditor (FITSP-A)
- Microsoft Certified Security Engineer (MCSE)
- Microsoft Certified Desktop Support Technician (MCDST)
- Microsoft Certified IT Professional (MCITP)
- Microsoft Certified Technology Specialist (MCTS)
- Microsoft Certified Systems Administrator (MCSA)
- GIAC Security Essentials Certification (GSEC)

Trusted Cyber Security Advisors and Practitioners for Federal Government and Commercial Clients

The Business of Cloud Services

EmeSec knows the business of cloud services. We help agencies align their cloud strategies with current policies and security requirements by brining forward credible and reliable security best practices, combined with creative ideas. EmeSec customers reap the benefits of more trustworthy, economical, scalable, on-demand and flexible computing.

Mobile & Wireless Computing

EmeSec offers information assurance services tailored to meet the evolving mobility needs of the government workforce. EmeSec services include strategy, policy, engineering, and security test & evaluation to ensure improved security for sensitive data stored on mobile devices including laptops, PDAs and/or smartphones.

Information Lifecycle Management

EmeSec provides full information lifecycle management support to protect and secure data and information during all stages of its life including creation, use, maintenance and disposal.

EmeSec Information Assurance / Cyber Security Services

Strategic Security Management

- Program Management Support
- Security Planning
- Risk Assessment and Mitigation
- Security Training and Awareness
- IV&V
- BPR

Provision & Evolve

- Information Assurance Compliance
- Enterprise Security Architecture, Design and Engineering
- System Requirements and Planning
- System Development
- Test & Evaluation
- Technology Demonstration

Operate & Maintain

- Information System Security Management
- Data Administration
- Network Services
- System Administration
- Systems Security Analysis
- Knowledge Management
- Technical Support

Protect & Defend

- Vulnerability Assessment and Management
- Penetration Testing
- Computer Network Defense
- Incident Response
- Infrastructure Support
- Investigative Forensics
- Cyber Threat Analysis

BD-TM-005

Selected Corporate Experience

Client/Industry	Project/Description	Our Value Add
Department of Veterans Affairs - Office of Cyber Security (Prime Contract)	**Information Assurance Technical Support Services:** FISMA M&O; Security & Policy Guidance; Enterprise Security; TOC; Privacy M&O.	Emerging technology assessment for information protection, comparative research and policy gap analyses.
Department of Veterans Affairs - OCIS (Prime Contract)	**Privacy Violation Tracking System (PVTS)**: TOC-Development and publication of a Privacy Awareness curriculum and film.	Curriculum coordination, script development, on location filming for computer based training.
Department of Veterans Affairs - Austin Automation Center (Prime Contract)	**General Support System (GSS) Certification & Accreditation:** Risk Assessment, Security Test & Evaluations, POA&Ms, System Security Plan, Security Assessment Report, Accreditation Letter, Certification Letter, and FIPS 199 Review.	Met a 60-day timeline for GSS C&A deploying a simultaneous testing methodology.
Department of Veterans Affairs – Office of Cyber Security (Prime and Subcontract)	**Security Documentation and Site Support Team**: Provide site-specific and major IT system information assurance analysis and documentation support. Gap analysis and remediation activities to ensure compliance.	Full security lifecycle support for a multi-node region-wide network with over 140 network servers in 7 geographically separated locations.
Department of Veterans Affairs – Office of Cyber Security (Prime Contract)	**Security Technical Management Services**: Provide enterprise-level IT security policy research, review, development, and maintenance support. Authored VA cloud policy.	Active participation in NIST IT security, mobile, and cloud technology working groups. Co-authorship on numerous NIST policy documents.

Selected Corporate Experience (continued)

Client/Industry	Project/Description	Our Value Add
Department of Veterans Affairs – Corporate Data Center (Subcontract)	**Privacy Program Management and Operation Documentation Assistance:** Privacy Impact Assessments (PIA), system security plans, configuration management plans, and contingency plans.	Delivered 12 PIA assessments and modified, developed, and delivered 75+ FISMA related documents in 6 month timeframe.
U.S. Naval Hospital – Jacksonville, FL (Prime Contract)	**Network / Systems Administration Security Support**: Network operations and management of LAN/WAN and AHLTA system application. Server Management (e-mail, print, exchange, Blackberry, Active Directory, SAN, NAS). Perimeter firewall management and IDS.	Full security lifecycle support for a multi-node region-wide network with over 140 network servers in 7 geographically separated locations.
U.S. Air Force Medical Operations Agency (Prime Contract)	**Medical Logistics Support, Contingency Operations Support**: Business processes, policies, procedures and support plans. Medical logistics acquisition strategies for War Reserve Materiel (WRM).	Coordinated alignment and integration of AFMOA requirements with overall contingency program requirements.
U.S. Air Force Medical Systems - Office of the Chief Information Officer (Prime Contract)	**IA Engineering and Support Services**: DoD Information Assurance Certification and Accreditation Process (DIACAP) Information Assurance (IA) engineering and analyst services. Lab management support.	Delivered layered approach that incorporates traditional and well-documented assessment & authorization (A&A) activities consistent with NIST, OMB and FISMA regulations.
DHS U.S. Coast Guard (Prime Contract)	**Technical & Financial System Review**: Process improvement identification. Systems documentation. Overall governance.	Optimized a 60-day time constraint providing executive briefs on system functionality, performance, and regulatory compliance.

Selected Corporate Experience (continued)

Client/Industry	Project/Description	Our Value Add
Department of Labor - Chief Information Security Office (Prime Contract)	**CISO Program Support Services**: FISMA and Privacy M&O, Security Policy and Guidance, Enterprise Security, Training, Outreach, and Communications (TOC).	Pragmatic security program technical support services integrating CPIC and EA.
Department of Labor - Occupational Safety and Health Administration (Prime Contract)	**Technical Assistance and General Support to the OSHA Deployment of GASP Software:** Software deployment, nationwide desktop and server software audits on the OSHANET LAN/WAN.	Designed actionable security services optimizing FISMA & NIST governance. Application Security best practices.
Federal Trade Commission – OITM Enterprise Security (Prime Contract)	**Enterprise Security Technology Assessment for Personally Identifiable Information**: Automated solution identification. Security software product review & evaluation. Product technical analysis and business case documentation.	State-of-industry PII monitoring, tracking and documentation; practicable key stakeholder involvement; and actionable alternative client-centric solutions.
Environmental Protection Agency – Senior Agency Info. Security Officer (SAISO) (Subcontract)	**SAISO Program Support**: Project management; policy, procedures, standards, and guidance; compliance; training; oversight and coordination; and reporting support.	Established stakeholder-driven program and mission support model, responsive to system-owner business needs. Performance measures and metrics-driven results.
Environmental Protection Agency – Office of Research and Development (Subcontract)	**Application Security Program Support**: Implemented new application security program. Provided program and application-level support. Developed Application Security Reporting & Requirements (ASRR) procedures, templates, and checklists.	Established transformation roadmap. Implemented structure where none existed, including establishing baseline inventory of applications.

BD-TM-005

Selected Corporate Experience (continued)

Client/Industry	Project/Description	Our Value Add
DOT Federal Aviation Administration – Cyber Security Management Center (Subcontract)	**FAA CSMC Support:** Staff analysts and duty officers provide support to FAA's CERT organization. Intrusion detection, vulnerability assessment, threat assessment, mitigation and reporting.	Near-real time assessment of threats. Support multiple Cabinet-level Federal Agencies. Packet level inspection of data.
U.S. Army Research Laboratory (ARL) – Army Materiel Command (Subcontract)	**Security Operations Center (SOC) Support**: Provide network operations security support. Research and analysis. Security test and evaluation. Security policy and procedures. Real-time and retrospective intrusion detection analysis.	Support Trusted Internet Connection (TIC) and EINSTEIN government initiatives. Ability to deliver qualified staff in hard-to-recruit regions.
DOD Pentagon Force Protection Agency (Subcontract)	**Information Assurance Technical Support Services:** Information assurance monitoring and alerting on all PFPA information systems.	Reactive and proactive defense assessment of current and envisioned future security attacks. Creation of actionable defense solutions.
General Services Administration – Federal Acquisition Service (Subcontract)	**GSA FAS Application Maintenance and Enhancement (GSA FAME) Support**: Web development and maintenance of FAS' auction purchasing website.	full information lifecycle management support to protect and secure data and information during all stages of its life.
U.S. Department of Agriculture-Forest Service (Subcontract)	**Enterprise-wide Security Procedures / C&A Compliance**: FIPS 200, NIST 800-53, and FISMA implementation. Security audit result improvement. Comprehensive information security controls program.	Managed and facilitated cultural change to new methods and approaches for IT security and security control documentation procedures.

Doing Business with EmeSec

Easy to Get to...

- 8(a) Program - sole source awards up to $4M
- SDVOSB Program - sole source awards up to $5M

Prime Contracts

- 8A STARS II - C1 FA4 (GS-06F-1021Z)
- GSA IT 70 Schedule (GS-35F-0027S)
- DHS PACTS FC 4
- eFAST MOA (DTFAWA11A-00050)
- OPM IT BPA - STA 3.3.4 (OPM32-12-A-0029)

Partner-Contracts

- ALLIANT SB
- VETS GWAC
- TSA IVV BPA
- USAMS II
- DoS SASI
- EPA ITS-BISS II
- SEAPORT E

Reference

- DUNS Number: 128976821
- Cage Code: 3EPT1
- NAICS Codes:
  - 541519, 541511,
  - 541512, 518210,
  - 519130, 541330,
  - 541430, 541611,
  - 541618, 541690,
  - 561110, 611420

Why EmeSec?

"Unlike other cybersecurity solutions providers, EmeSec doesn't subscribe to the myth that security/risk and innovation are mutually exclusive.

Our intuitive, adaptive and game-changing solutions are designed to thwart emerging threats and prepare our clients for the cybersecurity challenges of the future.

We focus on protecting information and strengthening the nation's security fabric so that agencies can focus on meeting their mission goals."

BD-TM-005

Contact Us

Maria C. Horton

CEO / President

mchorton@emesec.net

(703) 956-3036

Rod Volz

Vice President

rhvolz@emesec.net

(703) 956-3563 office

(703) 244-3892 mobile

EmeSec Incorporated
1818 Library Street, Suite 500
Reston, VA 20190

www.EmeSec.net