CAPABILITY STATEMENT

ENG - SURING DELIVERY OF QUALITY IT SOLUTIONS

ENG Solutions Inc.

www.EngSolutionsIT.com

POC: Hank Eng, President
(CISSP, CISM, CISA)

703.618.9670

hank@engsolutionsit.com

SBA 8(a) Certified Company

TS Facility Clearance

CAGE Code: 6Q0v1

Duns: 868849154

TIN: 27-4310571

COMPANY SNAPSHOT

- Cybersecurity consulting company founded in 2010
- SBA 8(a) certified company
- Past performances with DoD, DHS, and IC communities
- Top secret facility clearance
- NSA PISA Program participant

ENG SOLUTIONS NAICS CODES

519190	All Other Information Services
541512	Computer Systems Design Services
541519	Other Computer Related Services
541611	Administrative Management and General Management Consulting Services
541614	Process, Physical Distribution, and Logistics Consulting Services
541618	Other Management Consulting Services
541990	All Other Professional, Scientific, and Technical Services

ENG SOLUTIONS

CAPABILITY STATEMENT

ENG - SURING DELIVERY OF QUALITY IT SOLUTIONS

CORE COMPETENCIES

RISK & SECURITY	COMPLIANCE / AUDIT READINESS	SECURITY ASSESSMENTS
• Cyber Security • Enterprise and systems security • Security architecture • User security awareness training • Vulnerability management • Incident response • Risk management framework (NIST 800-37) • Continuous monitoring (NIST 800-137) • Information Assurance (C&A and DIACAP)	• FISCAM, A-123, A-130, SOX, FIAR support • Internal controls • Policies and procedures development • Financial statement audit support • FISMA support • Audit readiness support and training • Remediation support	• IV&V • Web / applications • Penetration testing (red teaming) • Security assessments (blue-teaming)

CURRENT / PAST CUSTOMERS

The United States Coast Guard (USCG) (Sub to DRC)

The Department of Homeland Security Infrastructure Protection (DHS IP) (Sub to SRA)

The Defense Intelligence Agency (DIA) (Sub to Accenture Federal Services)

The United States Army Information Technology Agency (USA ITA) (Sub to L3)

The Defense Logistics Agency (DLA) (Sub to KPMG)

Department of Defense (DoD) (Sub to CSRA)

Department of Agriculture (USDA) (Prime)

Government Accountability Office (GAO) (Sub to Acuity)

ENG SOLUTIONS

CAPABILITY STATEMENT

ENG - SURING DELIVERY OF QUALITY IT SOLUTIONS

SUCCESS STORIES

1. ENG Solutions supported the United States Army Information Technology Agency (USA ITA) Enterprise Security contract, ENG Solutions was charged with developing various security assessment and inspection programs. Collectively, the mission of these programs is to improve ITA's enterprise security posture and pass all mandated inspections. The establishment and execution of these programs had an immediate and positive impact. In 2012, ITA passed and scored higher marks during its Computer Network Defense Service Provider (CNDSP) Inspection. In 2013, ITA passed its Inspector General (IG) Information Assurance Inspection. Prior to this, ITA had failed its last five IG inspections spanning back to 2009. ENG Solutions takes great pride in being the driving force behind this success story.

2. ENG Solutions supported the United States Coast Guard (USCG) Audit Remediation contract, the team provided subject matter expertise in the areas of information systems audit, weakness remediation, process improvement, risk management, certification and accreditation (C&A), information assurance, and security continuous monitoring. Specifically, ENG Solutions developed corrective action plans to address security control issues identified by the external auditors (KPMG). In addition, ENG Solutions developed a continuous monitoring methodology that provided greater awareness and transparency in regards to information security controls and operating statuses. As a direct result of these activities, the USCG was able to resolve long-standing issues (repeat findings), decrease the number of identified findings (year-over-year), and had the "material weakness" aspect from the Financial Statement audit opinion removed.

3. ENG Solutions supported the Defense Intelligence Agency's Audit Readiness effort, ENG Solutions developed and presented a risk-based assessment approach which was approved by the contracting officer and government program manager. Once the approach was implemented, time and level of effort needed to assess each system was cut by more than 50% resulting in greater efficiency. This allowed the system owners more time to develop correct action plans (CAP) needed to remediate control weaknesses. ENG Solutions also developed a systematic approach to weaknesses remediation.

Core Capability Highlight #1 – Internal Controls / Security Solutions

Many security companies, specifically those with products to sell put great emphasis on external threats. They push boundary defense and security information and event management (SIEM) tools as the solution to all your information security woes. However, the facts is, any seasoned professional will tell you that the greatest risk to an organization's security program are the internal users (employees and contractors). What happens when those responsible for managing those controls and tools fail to do their jobs – risk to the organization increases! At ENG Solutions, we understand this. We have developed solutions and methodologies to address high impact areas such as access management and monitoring, user training, and security continuous monitoring (see core capability #3). We take the time to understand your issues, perform proper analysis (root, gap, cost, etc.), and develop appropriate solutions. Remember, not all problems require a fancy expensive automated tool.

ENG SOLUTIONS

CAPABILITY STATEMENT

ENG - SURING DELIVERY OF QUALITY IT SOLUTIONS

Core Capability Highlight #2 – Security Assessments

A security assessment can be defined as the execution of tests procedures (by an independent third party) to identify gaps, weaknesses, and vulnerabilities within an organization, system, application, or specific control. Security assessments can facilitate a heighten awareness and provide decision makers with critical information as it relates to the effectiveness of security controls, risk management, compliance, and enterprise security posture (see chart below).

ASSESSMENT DISCIPLINE	DESCRIPTION	MARKET OPPORTUNITIES
Penetration Testing (Red Teaming)	A penetration test (PenTest) is an authorized attack (hack) on a network / system with the goal of finding security vulnerabilities and possibly exploiting those vulnerabilities to determine its impact on the system, network, and organization. A penetration test may be a white box (where all background and system information is provided by the customer) or black box (where only basic or no information is provided). PenTests are often used to determine if a network and / or system is susceptible to various attacks.	Any industry where customer data, proprietary information, and sensitive mission data is being developed, collected, retained, and processed such as banking, retail, credit card, insurance, federal government, defense, intelligence, health, etc. Examples of requirements already in place where security assessment services are needed to ensure requirements are being met include: • Federal Risk and Authorization Management Program (FedRAMP) • Sarbanes Oxley (SOX) • Payment Card Industry (PCI) • Attestations (SSAE16) • Office of Management and Budget (OMB) A-123 • Federal Information Security Management Act (FISMA) • Federal Financial Management Improvement Act (FFMIA) • Health Insurance Portability and Accountability Act (HIPAA)
Technical Systems Assessment (Blue Teaming)	A collaborative (between client and third party assessor) technical assessment to identify vulnerabilities within various layers such as the network, operating system (OS), database, and application.	
Web Application Security Assessment	Uses dynamic and static code review to identify vulnerabilities within web-facing applications (accessible via the internet).	
Internal Controls Assessment	An assessment to determine the adequateness of design and operating effectiveness of the security and internal controls. This assessment focuses on internal mechanisms, processes, and procedures in place to protect information assets.	

While many companies focus on one or two of these disciplines, ENG Solutions can offer the entire security assessment suite to provide coverage across all layers of enterprise. This again leads to greater awareness and transparency regarding the current state of the organization's security posture which in turn allows the organization to better serve its clients and meet its business obligations (laws and regulations regarding privacy, financials, health, customer information, etc.).

Core Capability Highlight #3 – Security Continuous Monitoring

Security continuous monitoring is NOT simply deploying automated tools to defense against external attacks. As a matter of fact – the number of controls that can be automatically managed is limited in relation to the total number of NIST (National Institute of Standards and Technology) controls. NIST defines ConMon as: maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. NIST Special Publication (SP) 800-37, *Risk Management Framework (RMF)*, provides a structured and repeatable process for which to manage system and enterprise risks. The RMF consist of six steps: (1) categorize system, (2) select security controls, (3) implement security controls, (4) assess security controls, (5) authorize system, and (6) monitor security controls. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, is focused on and expounds upon step 6 of the RMF – monitor security controls.

While the concept of ConMon is not new, at this point, adaptation and implementation across federal and DoD agencies is relatively limited. Additionally, most implementations are executed at the system level. In other words, individual system owners assign resources (ISSO, IAM, IAO, PM, administrators, etc.) on a system by system basis; therefore control monitoring is also performed on a system by system basis. However, to achieve coverage across the entire organization while also achieving efficiency and cost savings, ConMon should be implemented at the enterprise level covering all mission critical systems and high impact control areas utilizing a risk-based approach.

ENG Solutions has developed and deployed continuous monitoring programs for multiple agencies including Army ITA. Core components of the program include: gaining leadership support (via a program charter), developing appropriate standards & procedures, documenting a comprehensive list of systems & controls, developing meaningful metrics, implementing automated tools (for transparency and efficiency), performing root cause analysis, performing lessons learned exercises, utilizing POA&Ms and risk exceptions, developing practical remediation strategies, implementing effective communication plans, and providing on-going training to personnel and stakeholders. Through our ConMon program, ITA has reaped the following benefits:

- Improved compliance with DoD and Federal mandates such as the Federal Information Security Management Act (FISMA)
- Achieved greater visibility into control design and operating effectiveness
- Ability to provide senior leadership with information needed to make risk management decisions
- Implemented corrective actions and process improvements resulting in a strengthen security posture

CAPABILITY STATEMENT

ENG - SURING DELIVERY OF QUALITY IT SOLUTIONS

Core Capability Highlight #4 – Information Technology / Systems Auditing

From RFP responses to delivery, ENG Solutions has supported many auditing engagements to include: United Stated Coast Guard Audit Remediation, Defense Logistics Agency Financial Improvement and Audit Readiness (FIAR), Defense Intelligence Agency FIAR, Department of Defense Education Activity FIAR, and Department of Transportation Financial Statement Audit. Additionally, ENG Solutions has developed and implemented various audit methodologies and strategies (risk based testing, root cause analysis, systematic remediation approach, etc.) in support of FIAR, FISCAM, A-123, A-130, FISMA, and SOX engagements.