



**Mark Marsh**  
 4400 STATE HWY 121 STE 300-1265  
 LEWISVILLE, TX 75056 USA  
 mark@msmnetsecurity.com  
 (312) 952-8900  
**www.msmnetsecurity.com**

## COMPANY DATA

<b>CAGE Code</b>	<b>8CDL5</b>
<b>UEI Number</b>	<b>WCFDLHXL5KL8</b>
<b>GSA SIN (Cybersecurity)</b>	<b>54151HACS</b>
<b>GSA MAS</b>	<b>#47QTCA22D006Q</b>
<b>SBA 8(a)</b>	<b>EXP: 03/23/2030</b>
<b>STARS III</b>	<b>#47QTCB22D0526</b>
<b>SAM Registration</b>	<b>Active</b>
<b>State of Texas HUBZONE</b>	<b>Yes</b>
<b>Accepts Government P-Cards</b>	<b>Yes</b>
<b>Service Area</b>	<b>Nationwide</b>
<b>State of Illinois BEP/MBE</b>	<b>IPHEC-2140</b>

## NAICS CODES

<b>541511</b>	<b>Custom Computer Programming Services</b>
<b>541512</b>	<b>Computer Systems Design Services</b>
<b>541513</b>	<b>Computer Facilities Management Services</b>
<b>511210</b>	<b>Computer Software</b>
<b>423430</b>	<b>Computer Hardware</b>
<b>611420</b>	<b>Computer Training</b>
<b>611430</b>	<b>Professional and Mgmt. Training</b>

## PAST PERFORMANCE

**Genuine Parts Company**  
 Work performed: GRC Software Implementation

**NAPA AUTO PARTS**  
 Work performed: SOC Program Development

**Assurant**  
 Work performed: Development and implementation of a Rsam Risk Management System

## STAFF CERTIFICATIONS

<b>PCI SSC</b>	<b>CSA</b>	<b>AWS</b>
• PCIP	• CCSKv4	• AWS Certified
	• CCAK	
<b>ISC2</b>	<b>GASQ</b>	<b>Red Team Security</b>
• CISSP	• ISO/IEC 27001	• Social Engineering Experiment
• CCSP	• ISMS Lead Auditor	
<b>ISACA</b>	<b>DRII</b>	<b>CISCO SYSTEMS</b>
• CISA	• MBCP	• CCNA R&S
• CRISC	• CBCLA	• CCDA R&S
• CDPSE	• Healthcare	• CCNP R&S
• CISM	• CHPSE	
• ISACA	• Medical Fraud	<b>PMI</b>
<b>JUNIPER</b>	• Texas HB 300	• Completed PMP Training via PMI
• JNCIA-JUNOS		

## HARDWARE & SOFTWARE SERVICES

- Systems**
- IBM POWER and STORAGE
  - DESKTOPS & WORKSTATIONS
  - NOTEBOOKS & TABLET PCS
  - TABLETS & EREADERS
- Software**
- SECURITY
  - VIRTUALIZATION
  - UTILITIES
- Networking**
- SERVICES/SUPPORT
  - STORAGE
  - WIRELESS PRODUCTS

## CORE COMPETENCIES

- Cyber Defense
- Vulnerability Management Penetration Testing
- Governance, Risk and Compliance
- PCI and HIPPA Security Assessments
- IT/HEALTHCARE Staffing
- Security Awareness Training
- Managed Security and Monitoring Services
- Identity Validation Technology

## DIFFERENTIATORS

Over 30 years of proven Information Technology industry experience in both private and public sectors.

- Innovative
- Performance Driven

We listen to your unique requirements and tailor our cost-effective solutions to deliver measurable results.

- Flexible

Our focus is working cohesively toward delivering exceptional solutions that outperform client expectations.

- Valued Partner

One company with multiple, independently-rated, best-of-breed services, Fortune 500 Cybersecurity/GRC Project experience.



## **Past Performance # 1**

**Customer:** Genuine Parts Company

### **Description of work performed: GRC Software Implementation**

Designing Database SQL queries, Process Workflows and custom reports and training of end-users. Our Role including providing the delivery consultant and overall engagement management for the Development and implementation of a Governance, Risk and Compliance (GRC) Management System. Our development automates the workflows involved with the adherence to government and industry compliance regulations. Companies that are in compliance have a reduced risk of Cyber-attacks and data breaches.

#### **Tasks include:**

- Requirements gathering – Five day on-site in-depth discussion with process owners and stakeholders to collaborate, brainstorm, knowledge share and define specific requirements for a solid risk management process in alignment with company maturity, resources, and compliance requirements.
- Documentation of Client Company requirements and deliverables with follow-up meetings to ensure mutual agreement.
- Building of GRC system to align with process requirements, company terminology, existing processes, culture and level of maturity.
- Training & testing with process managers to ensure system functionality and interface in line with requirements, and to identify issues and new unexpected requirements.
- Second phase of building, training and testing to ensure process managers acceptance of system and process.
- Roll out to end users with communication plan, training and on-going support while process and system is integrated into daily responsibilities.
- Initial project completion was marked by measurable increase in the level of maturity of the GRC program and the specific process developed. Ongoing customization continues.

**Dollar value of project:** \$1,000,000 Plus (Master Services Agreement)

**Period of performance:** 01/01/2019 – 06/30/2022

## **Past Performance # 2**

**Customer:** NAPA AUTO PARTS

### **Description of work performed: SOC Program Development**

We leveraged our expertise in Security Operation Center (SOC) Technologies and Operations by performing the following functions: Investigate Incident Response (IR) events/alerts reported from Splunk SIEM NSM, Firewall, Rackspace hosting, Splunk Security Analytics.

- Participated in Network threat intelligence collaboration with other business units by sharing indicators or compromise, and attack data.
- Perform threat hunting exercises to find advance persistent threats on the Network using Splunk Security Analytics.
- Designed templates in Splunk Security Analytics to have relevant meta groups and have a logical/targeted approach for investigations
- Created and defined custom syslog template in in Splunk Security Analytics and integrated to Splunk SIEM.
- Analyzed packets more in depth by using Wireshark.

**Dollar value of project:** \$1,000,000 Plus (Master Services Agreement)

**Period of performance:** 01/01/2019 – 06/30/2022



### **Past Performance # 3**

**Customer:** Genuine Parts Company

**Description of work performed: Global PCI Pre-Assessment for Report on Compliance (ROC)**

Successfully designed and led a global data, privacy, and Cybersecurity compliance program across nine (9) countries from greenfield including PCI, SOC, GDPR, CCPA. Implemented global c-suite governance, led third party assessments and certification.

**Dollar value of project:** \$1,000,000 Plus (Master Services Agreement)

**Period of performance:** 01/01/2019 – 06/30/2022

### **NAICS CODES**

MSMNET Security has capabilities in **SIN:** 54151HACS **NAICS:** 541511, 541512, 541513, 541990.

We specialize in Integrated Risk Management, Vulnerability Management and Compliance centric services. Our CISO Advisory-Level Staff have numerous Certifications/Accreditations such as:

### **STAFF CERTIFICATIONS**

#### PCI SSC

- QSA (Qualified Security Assessor) Teaming Partner
- PCIP (Payment Card Industry Professional)

#### ISC2

- CISSP (Certified Information Systems Security Professional)
- CCSP (Certified Cloud Security Professional)

#### ISACA

- CISA (Certified Information Systems Auditor)
- CRISC (Certified Risk and Information Systems Control)
- CDPSE (Certified Data Privacy Solutions Engineer)
- CISM (Certified Information Security Manager)
- ISACA Certified Training: Cloud Computing Security & Audit



## STAFF CERTIFICATIONS CONTINUED

### AWS

- AWS Certified Cloud Practitioner

### CSA (Cloud Security Alliance)

- CCSKv4 -
- CCAK

### GASQ

- ISO/IEC 27001 ISMS Lead Auditor

### DRII (Disaster Recovery Institute International)

- MBCP (Master Business Continuity Professional)
- CBCLA (Certified Business Continuity Lead Auditor) (ISO 22301 Lead Auditor) – Current
- Healthcare/Medical
- CHPSE (Certified HIPAA Privacy Security Expert)
- Medical Fraud, Waste and Abuse Certification
- Texas HB 300 Certification

### Red Team Security Training

- Social Engineering Expert

### CISCO SYSTEMS

- CCNA R&S
- CCDA R&S (Network Design/Architecture)
- CCNP R&S

### JUNIPER

- JNCIA-JUNOS

### PMI (Project Management Institute)

- Completed PMP Training via the PMI





## State/Federal Services

- FISMA
- FedRAMP (SSP's, POAM's, SAR's, SAP's, RAR's)
- CMMC / NIST 800-171
- StateRAMP
- HIPAA

## PCI-DSS

- SAQ scoping & completion
- PCI-DSS Gap Assessment, Readiness Assessment, Road-Mapping, Cardholder Data Environment (CDE) Scoping
- On-Site Assessments
- Logical Testing (Internal/External Vulnerability Scanning & Segmentation Testing)

## Compliance Services

- CIS 7.0 & 8.0
- NIST-CSF, NIST 800.53, NIST 800.171 (we can audit to the bulk of the NIST SP's)
- CMMI
- ISO 27001/27002 Information Security Management Systems (ISMS)
- ISO 9001 Quality Management Standard (QMS)
- SOC 2 Type 2 Gap Assessment, Readiness Assessment, Road-Mapping
- HIPAA
- PCI-DSS

## Physical & Logical Security Services

- Penetration Testing
- Internal Vulnerability Scanning
- External Vulnerability Scanning
- Network Segmentation Testing
- Database Vulnerability Scanning
- Application Security Testing
- Web Application Testing
- Secure Code Review
- Red Team Operations (Physical PenTesting)
- On-Site Physical Security Assessment

## Cloud Services

- CSA Cloud Controls Matrix (CCM) / CAIQ
- Security/Architectural Review