**McSOC Statement of Objectives**

**November 15, 2016**

**1.0 Overall Objectives:**

The overall objective of the McSOC Network Reference Architecture (McSOC) is to produce a reference network system that includes all the elements needed to exercise the full functionality of a Security Operations Center as a component of a resilient network infrastructure. The complete McSOC architecture includes sensors embedded in the internal components of a enterprise architecture including enterprise servers, enterprise workstations, and a segmented enclave network modeled here as a development network. The system will include automated reporting of the status of the deployed network.

**2.0 Licensing Objectives:**

The following additional information is provided for project clarification:

1. This reference architecture will be built entirely of open source components.
2. This reference architecture will have the ability to swap out components with commercially licensed components in any particular deployment.

**3.0 Engineering objectives:**

1. Design, develop, integrate, test, deliver, install and support a high fidelity SOC to provide a reference SOC architecture for capability definition, requirements analysis, network attack simulation, testing, and training.
   1. Incident Handling Process
      1. Security Operations Management
      2. Asset Management
      3. Endpoint Security Policy Management
      4. Security Ticket Workflow
      5. Logger Manager
      6. Intrusion Protection Manager
   2. Monitoring & Threat Management
      1. Intelligence Management
      2. SIEM Manager
      3. Malware Scanning Service
      4. Threat Managerment Service Database
   3. Host Forensics & Malware Analysis
      1. Digital Forensics
         1. Incident Response Lifecycle
         2. Data Collection
         3. Analyst Skills
         4. Forensic Toolsets
         5. Anomaly Recogintion
      2. Malware Analysis
         1. Acquisition Strategy
         2. Metadata Extraction
         3. Static Indicators
         4. Behavior Analysis
         5. Categorization and Attribution
         6. Reverse Engineering
   4. Full Packet Capture Network Forensics
      1. Network Tap
      2. Network Storage
      3. Network Manager
      4. Network Malware Analysis
   5. Security & Audit Operations
      1. Event and Syslog Collection
      2. Penetration Testing
      3. Patch Management
   6. Vulnerability Assessment
   7. Software Vulnerability Scanning
      1. Network Service Scanning
      2. Identity Management
   8. Active Directory Domain Controller
      1. Network Authentication Server
      2. PKI Management
      3. Two Factor Authentication
   9. Desktop and Server Controls
      1. Security Configuration Scanning
      2. File System Integrity
      3. Anti-Virus Management
2. Use a visualization abstraction layer to allow deployment on multiple visualization platforms.
3. Use open source components.
4. Develop and document procedures for executing the SOC functions. Manage the McSOC network in accordance with these procedures.

**4.0 Program Objectives:**

1. Self deploying reference architecture can be used as a model for capability definition, requirements development, and product selection.
2. Self deploying reference architecture can be used for training and emulation.
3. Self deploying reference architecture can be used for simulation and network testing.

**5.0 Logistic Objectives:**

1. No sustainment activities are planned at this timeouts
2. Perimeter
   1. firewall/vpn
   2. ids/ips
   3. utm
   4. gateway
   5. datacenter
   6. dlp
3. Content
   1. endpoint
   2. AV
   3. Web
   4. URL Filtering
   5. Mail Security
   6. Application Security
   7. Analytics
4. Policy Compliance
   1. Device Security
   2. End User Security
   3. Log Analysis
   4. Event Management
   5. Reporting
   6. Identity and Access Management
5. TFA
   1. Authenticaion
   2. Encryption
   3. Federation
   4. SSO
6. Management
   1. Incident Mgmt
   2. Change Mgmt
   3. Asset Mgmt
   4. Vulnerability Management
   5. Patch Managment