SURVICE ENGINEERING COMPANY

INFORMATION ASSURANCE/ CYBERSECURITY SERVICES

CYBERSECURITY

Providing cybersecurity and the defense of cyberspace is essential to mission success for our warfighters, requiring operational, tactical, and strategic planning. The importance of cybersecurity on and off the battlefield demands that significant emphasis be placed on the capability to protect information systems operating in cyberspace and the ability to provide data confidentiality, integrity, and availability.

The warfighter's confidence in having secure reliable information and communication is a fundamental step toward mission success. Secure command, control, communications, and situational awareness are critical throughout the Global Information Grid, at every level. Any loss, degradation, or corruption of this information threatens the mission's survivability, integrity, and ultimately the warfighter. The protection of information transmitted, received, or stored by information systems is mandated by Congress and the DoD.

The SURVICE Engineering Company has been identifying and mitigating combat system and process vulnerabilities for more than 30 years. SURVICE's cybersecurity engineers and analysts have the knowledge, expertise, and industry recognized certifications to help ensure safe and secure dissemination of critical information in today's network-centric warfare environment.

CYBERSECURITY SERVICES

CYBERSECURITY COMPLIANCE SUPPORT

SURVICE has supported DoD program compliance with:

- The DoD Information Assurance Certification and Accreditation Process (DIACAP)
- DOT&E Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs
- DoD Instruction 8510.01, Risk Management Framework for DoD Information Technology (IT)

CYBERSECURITY ASSESSMENT

SURVICE has provided support in the areas of:

- Security Posture Assessment
- Vulnerability Resolution
- Operational Impact Analysis

CYBERSECURITY ASSESSMENT

SURVICE has:

- Developed detailed test plans
- Developed cybersecurity data collection documentation
- Analyzed DIACAP scorecard and supporting cybersecurity/IA artifacts
- Analyzed documentation in support of DIACAP to RMF transition
- Provided data analysis of Threat Computer Network Operations (TCNO) and Protect, Detect, React, Restore (PDRR) test events
- Supported cybersecurity evaluation at US Army Network Integration Evaluation (NIE) rotations
- Developed cybersecurity evaluation input to System Evaluation Plans (SEP), Operational Test Agency (OTA) Evaluation Reports (OER), OTA Milestone Assessment Reports (OMAR), and Emerging Results Briefings (ERB)
- Understanding of current DOT&E and DASD (DT&E) cybersecurity policy and guidance

Mr. Steve Clifford: 410-273-7722, x363 | stevec@ survice.com