



DEPARTMENT OF TREASURY

Avineon TIPPS-3 Contract

BEP SECURITY CONTRACT

The Office of Critical Infrastructure and IT Security awarded a contract in October 2007 to Avineon and Global Network Systems (GNS, Inc.), a security and network-based IT services company located in Rockville, Maryland. GNS specializes in leveraging technology to improve business productivity.

GNS, Inc. provides objective and knowledgeable analysis of IT security policy, systems documentation and IT security management issues, as well as certification and accreditation (C&A) and compliance monitoring.

GNS has a Top Secret facility clearance as well as cleared and certified professionals.

CONTRACT SCOPE

- Review and analysis of IT security policy, systems documentation and IT security management
- C&A projects and compliance monitoring
- Technical, analytical and program management support
- Recommendation and documentation standards for implementing security controls
- Development of Security Test and Evaluation (ST&E) plans
- Administration and support for security analysis, incident support and management
- Audit of IBM Mainframe, LAN/WAN and other systems
- IT Contingency Plan Testing Support



GLOBAL NETWORK SYSTEMS

Discovering New Solutions, Each Day

1 RESEARCH COURT, SUITE 340
ROCKVILLE, MARYLAND 20850
PHONE: 301.921.4GNS (4467)
FAX: 301.921.0309
EMAIL: INFO@GNS-US.COM
WORLDWIDE: WWW.GNS-US.COM

IT PROGRAM SECURITY SUPPORT BUREAU OF ENGRAVING AND PRINTING

BENEFITS

- Negotiated rates for the life of contract
- On-site staff
- Covers the entire scope of IT security

TASK AREAS

- Security Program Management Support
- C&A Support
- IT Security Operations Support
- IT Security Awareness Training Support
- Security Compliance Monitoring Support





TASK AREA 1: Security Program Management Support

- Assist in developing IT security policies and procedures; identify policy and procedural gaps; assist in recommending, writing, and updating policies and procedures
- Recommend and document configuration standards and standards for implementing security controls
- Recommend strategies and tools to monitor and report FISMA compliance and manage remediation efforts, including: compliance with configuration standards; management of Plan of Actions and Milestones (POA&Ms) to identify, prioritize, and monitor all identified weaknesses, vulnerabilities, and deficiencies; and annual security control tests
- Assist in recommending and implementing solutions

TASK AREA 2: Certification and Accreditation Support

- Support the ISSO in: assessing systems and preparing security documentation; risk assessments; identification of security controls; preparation of security plans, interconnection security agreements and privacy impact assessments
- Develop security test and evaluation (ST&E) plans; conduct ST&E testing, analysis, and reporting; recommend additional security controls; prepare POA&Ms; draft Security Assessment reports, and C&A letters

TASK AREA 3: IT Security Operations Support

- Continuously monitor industry security trends; document and report on services
- Perform feasibility studies for the implementation of new technologies
- Administer and support security analysis, monitoring, and defense (IDS, IPS, firewalls, etc.); conduct security testing for all new and upgraded security equipment, networks, software, and services
- Implement immediate measures to react to identified security incidents and take actions to isolate and minimize negative impacts
- Install security patches; provide firewall management services; develop policies and standards for Intrusion Detection/Prevention Services; conduct security vulnerability scans

TASK AREA 4: IT Security Awareness Training Support

- Provide ongoing online security awareness training for policies, standards, procedures, and threats via initial instructor-led classroom training; includes final training plan and user guides

TASK AREA 5: Security Compliance Monitoring Support

- Audit IBM Mainframe, LAN/WAN, and other systems; perform continuous monitoring to ensure security controls remain effective; and provide IT Contingency Plan Testing Support