Cyber Security Analyst

- Job Title: **Cyber Security Analyst**
- Alternate Job Title: **Business Sys Anst Prin**
- Job ID: **10430BR**
- Posting Date: 2015-05-12
- Travel Percentage: 10%
- Location: **Washington, DC 20374-5127**
- US Citizenship Required: **Yes**
- Shift: **1st Shift**
- Required Security Clearance: **Secret**

Job Description:

The Information Assurance (IA)/Cybersecurity Analyst is responsible for providing Information Assurance, Cybersecurity, and Information Management to the Strategic Systems Program Command Information Officer (CIO).

Duties include the following:

Assist in conducting internal audits of SSP Enterprise IT networks, systems, applications, and security tools to ensure they adhere to SSP, Navy, and DoD security policies and procedures (e.g., STIGs, CTOs, IAVMs, FRAGOs, NTDs, etc.) and applicable frameworks and regulations (e.g., NIST, FISMA, etc.).

Review DoD, DON cyber security alerts, notices, IAVMs, etc., and conduct risk assessments and mitigation strategies when applicable.

Review security and data/logs to respond to security incidents on SSP Enterprise systems.

Support the SSP IAM/ISSM in developing SSP Cybersecurity standards and policies.

Maintain the SSP Enterprise systems certification and accreditation (C&A) plans; C&A topologies; ports, protocol, and services lists; contingency plans, disaster recovery procedures, incident response plans, and POA&M.

Provide technical guidance to the SSP IAM/ISSM, CIO, Cybersecurity Workgroup (CSWG), Program Managers (PMs), Program Management Officers (PMOs), FBM Partners, etc. on cybersecurity matters and initiatives, including researching new technologies to counter evolving threats.

Required Skills and Education:

Candidates must ensure that resume addresses all stated requirements of the posted requisition. Only resumes that specifically include all required skills/experience/education, will be considered.

Active DoD Secret security clearance
Bachelor's degree in Engineering, Information Systems, Computer Science or related field, preferred, but depending upon experience. will consider other degree disciplines and at least 8 years of professional work related experience, including at least 5 years experience supporting and/or maintaining information security technologies
Security-related industry certification
Experience with information security best practices and security frameworks
Knowledge and understanding of security technologies including intrusion detection/prevention systems, firewalls, vulnerability scanning, and data protection/encryption systems
Familiarity with network security tools and technologies including networking protocols
Experience developing policies, procedures, and technical training materials
Excellent verbal and written communication skills

Preferred Skills and Education:

Highly desired skills/experience:

Master's Degree in relevant field

About BAE Systems Intelligence & Security:

BAE Systems is a premier global defense and security company with approximately 90,000 employees delivering a full range of products and services for air, land and naval forces, as well as advanced electronics, security, information technology solutions and customer support and services. Information Solutions, based in Reston, Virginia, is among the 10 largest IT providers to the U.S. government, serving most of the federal defense and civilian marketplace. It provides network-centric command, control, computing, and intelligence (C3I) solutions; wideband networking radio systems; information systems for the U.S. intelligence community; geospatial information services; and information technology services. Leveraging its knowledge of signals and data derived from signals, Information Solutions has attained a market-leading position in advanced information technology research, intelligence analysis and production, and geospatial exploitation software. People are the greatest asset in any Company.

BAE Systems is committed to hiring and retaining a diverse workforce. We are proud to be an Equal Opportunity Employer, making decisions without regard to race, color, religion, sex, sexual orientation, gender identity, gender expression, marital status, national origin, age, veteran status, disability, or any other protected class.