Downloaded from <https://www.velvetjobs.com/job-descriptions/information-assurance-specialist>

# Example of Information Assurance Specialist Job Description

Our company is looking to fill the role of information assurance specialist. To join our growing team, please review the list of responsibilities and qualifications.

## Responsibilities for information assurance specialist

* Responsible for preparing documentation such as Risk Assessment Reports (RARs) for the ISSM/CISO, System Security Plans (SSPs), Development of Plan of Action & Milestones (POA&Ms) to ensure compliance with Government and DC3 Cybersecurity policies and procedures
* Define the NGA Enterprise ICD 503, Intelligence Overlay C modernization and transition roadmap for Infrastructure Services, NGA’s Enable GEOINT competency
* Assess NGA contract baselines against ICD 503, Intelligence Overlay C and compartmented functional and security needs for Infrastructure Services, NGA’s Enable GEOINT competency
* Define and control requirements for NGA systems and services to resolve gaps against compartmented functional and security needs, specifically ICD 503 Intelligence Overlay C requirements for Infrastructure Services, NGA’s Enable GEOINT competency
* Must perform daily reviews of systems to ensure normal maintenance functions are performing properly execution of daily/weekly system health checks/checklists
* Will coordinate with vendors, DISA, and NAVSEA, , component organizations for technology, capability, and policy issues
* Perform assessment of present levels of cyber security, define acceptable levels of risk, train all personnel in proper cyber hygiene and establish formal maintenance procedures
* Perform privacy impact assessments and provide PII data security and monitoring and migration strategies
* Identify potential vulnerabilities to cyber and
* Provide technologies for identification, modeling, and predictive analysis of cyber threats

## Qualifications for information assurance specialist

* Knowledgeable of current Government Information Assurance and Cybersecurity policy, regulations and standards
* Bachelor’s Degree Computer Science, Systems Engineering, Cybersecurity, Information Technology or related area, or the equivalent combination of education, professional training, or work/military experience
* At least 8 years of related experience to include previous SOC Analyst experience at a federal agency
* Bachelor's Degree with 5 years specific work experience and 8 years general work experience, preferred
* Or a high school diploma 7 years specific work experience and 12 years general work experience
* 3 years experience in conducting information system security assessments