# Application Security Specialist

AlphaSix is looking for an Application Security Specialist. Applicant must be knowledgeable and have experience with the Risk Management Framework (RMF) and be knowledgeable of the relevant NIST Special Publications guidance as it pertains to the Risk Management Framework (RMF).

## Clearance Requirement

Must be a US citizen.

## Location

Atlanta, GA

## Roles & Responsibilities

- Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
- Ensures that deployed applications are compliant with existing information security regulations, policies, and standards through regular testing against measurable metrics. Assists in preventing incidents by acting during design, development, deployment, upgrade, maintenance, and responds by finding, fixing and preventing security vulnerabilities.
- Applicant must be knowledgeable and have experience with the Risk Management Framework (RMF) process to include a working knowledge of the various steps/stages within the process.
- Applicant must be knowledgeable of the relevant NIST Special Publications guidance as it pertains to the RMF - specifically the NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) moving towards 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).
- Applicant must be able to participate in all Cybersecurity/IA Activities, including but not limited to ACAS & SCAP Compliance system vulnerability scanning, RMF A&A process, security authorization package training and processing, architectural diagram and viewpoint review, and package validation.
- Provide security policy interpretation, research, and development; information systems security; information technology research and analysis work; cyber security planning and implementation; industrial security work; information technology policy/guidelines development; and information security work.
- Applicant must have strong verbal and written communication skills and be detail-oriented.

## Required Skills

- Documented knowledge of the policies, instructions, regulations, and guidance of the National Institute of Standards and Technology, the Committee on National Security Systems, and the Director of National Intelligence. Specifically, the following:
    - Knowledge of FISMA, OMB-A130, and NIST security standards.
    - Experience with conducting systems evaluations/audits is a plus.

- Documented skill in the application of Security Assessment and Management tools. Specifically, the following:
    - GRC - Archer or Trusted Agent
    - Reviewing Scan Results from HP Fortify, BigFix, Tenable Nessus
    - Jira or ServiceNow experience is a plus.
- Experience promoting awareness of issues among management and ensuring sound security principles are reflected in organizations' visions and goals.
- Experience with conducting systems evaluations, audits, and reviews; documentation demonstrating the development of systems contingency plans.
- Experience in incident detection, analysis, coordination, and response; auditing systems, database, and applications; vulnerability assessments and compliance monitoring; experience in vulnerability assessments.
- Working knowledge of computer hardware (PDA, desktop, server, and peripherals), operating systems, applications, and databases (single user through enterprise); knowledge of information security products, regulations, standards, and guidelines.
- Experience in network monitoring; experience with incident response handling; sound knowledge of incident response handling policy and procedures; and knowledge of intrusion detection systems and other information security products, regulations, standards, and guidelines.

## Qualifications & Education

- A degree in Computer Science, Information Systems, Engineering, Mathematics, Business, or other related discipline is preferred. This position requires seven (4) years general database experience, four (4) years database administration/development experience for large complex databases; and two (2) years information technology experience.
- At least Four (4) years' experience in the integration and implementation of policy, regulations, and doctrine in telecommunications and information technology development.
- At least Four (4) years' experience in using security policies, standards, procedures, guidelines, and best practices from areas such as FISMA, NIST, and NSA.
- At least Four (4) years' experience integrating, developing, or deploying security products in enterprise level technology upgrades.
- DoD 8570/5239 IAT Level 2 Certification (Security + CE) or IAT Level 3 Certification (CASP or CISSP) is a plus.

## About AlphaSix Corporation

AlphaSix Corporation is a Washington, DC-based small business that provides Federal, state, and local governments with a broad range of IT products, solutions, and services focused on the convergence of big data and cyber security. At AlphaSix, we pride ourselves in providing a highly energized work environment where our employees are rewarded with competitive compensation packages and excellent benefits. We understand that to attract the top talent in the industry and provide the highest level of satisfaction to our customers, we need to provide an environment that supports our employees in their efforts to fulfill the needs of their clients and allows them to reach their fullest potential. AlphaSix offers a variety of benefits including competitive compensation, health insurance, disability coverage, 401(k) with matching program, paid holidays, and PTO.