INFORMATION SECURITY ANALYST IN WASHINGTON, DC

Job Description

Information Security Analyst

Washington, DC

Overview:

IP is looking for an Information Security Analyst with mastery level knowledge of IT security risk management activities under the Risk Management Framework (NIST 800-53, etc.).

Responsibilities:

The successful candidate will work with the contractor team and government customers to determine, and develop, an approach to information system security solutions to meet published security requirements. The position requires strong critical thinking and analytical skills, attention to detail, and excellent oral and written communication skills:

- Develop and/or analyze Judiciary information system security plans that conform with Judiciary Information Security Framework - JISF (based on NIST 800 Series Special Publications.)
- Help with day-to-day activities of the vulnerability management program at AOTO. (communication with stakeholders, PoA&M management)
- Use CSAM as a Security Assessment & Authorization (SA&A) management tool.
- Utilize technical expertise of computer security theories, principles, practices, and functional tools for a broad range of computer security related areas, including certification and accreditation of government information and telecommunications systems, IT disaster recovery and business continuity planning, and risk management for the Judiciary's IT systems.
- Ensure the integration of IT programs and services as required; and develop solutions to integration interoperability issues.
- Develop and implement new approaches and procedures regarding security measures that are in compliance with Judiciary and AOTO policies and guidelines.
- Work with other program offices, internal and external customers throughout the information system life cycle process to ensure adequate security considerations are built into systems in accordance with applicable Judiciary guidelines (1) to protect

the Judiciary systems and data assets, and (2) to ensure the continual review and implementation of information security training requirements throughout the life cycle process.

- Use vendor descriptions, technical documents and/or hands-on evaluation of applications to evaluate security controls, and will work with Subject Matter Experts (SMEs), developers, network engineers and network support personnel as necessary to obtain additional information required for adequate analysis.
- Maintain a current awareness of state of the art developments in INFOSEC standards, principles and policies.
- May serve as the AOTO-IT Security representative to meetings of various working groups, committees and or teams to represent AOTO INFOSEC requirements for systems software and hardware. To effectively represent AOTO IT Security in these meetings, the candidate must maintain current knowledgeable of Judiciary and AOTO's security architecture and evolving security requirements.
- Meet and collaborate with all levels of management within AOTO, and other program offices, and their employees and groups.
- Serve as an INFOSEC Analyst with responsibility for ensuring the confidentially, integrity, and availability of information and information systems supporting Judiciary assets through the planning, analysis, development, implementation, maintenance, and enhancement of information system security programs, policies, procedures, and tools.
- Provide expertise on AOTO's IT security architecture; emerging technologies and their applications to business processes; IT security concepts, standards, and methods; project management principles, methods, and practices including developing plans and schedules, estimating resource requirements, defining milestones and deliverables, monitoring activities, and evaluating and reporting on accomplishments.
- Perform other duties as assigned.

Qualifications:

Job Requirements

- At least 3 years at a Federal Agency (preferably Executive Branch) working with FISMA as a Risk Management Framework SME
- At least 8 years of progressive Information Technology (IT) experience including at least Five (5) years' experience in IT security, including C&A and/or IT security risk analysis, preferably in support of the Federal Government
- Mastery level knowledge of techniques, principles and theories pertaining to providing security and protection to IT resources.

- Mastery level knowledge of information systems security standards such as NIST and Federal Government requirements, as well as: industry best practices, standards and guidelines involved with the protection of hardware, software, and telecommunications equipment and services, to accomplish Security Assessment & Authorization activities.
- Mastery level knowledge of methods for protecting information systems and data; detecting and analyzing anomalous activity; restoring the security of information systems, network services and related capabilities; and identifying and mitigating information system vulnerabilities to prevent inadvertent data disclosure, unauthorized data modification, data destruction, or denial of service.
- Knowledge of methods and tools used for risk management and the mitigation of risk for information systems and data. This requires a technical mastery of, and hands on experience using, risk assessment methods to determine vulnerabilities in local environments, processing procedures, personnel and other system components.
- Technical understanding of integration of IT programs and services in a multi-location Wide Area Network; and the security controls, tools and techniques used to secure multiple platforms and operating systems through channels offering differing levels of trust and reliability.
- Knowledge of the operating characteristics of various operating systems.
- Knowledge of general management and auditing techniques for identifying problems, gathering and analyzing pertinent information, forming conclusions, developing solutions and implementing plans consistent with management goals.
- Mastery level knowledge and experience applying government standards, including NIST Risk Management Framework, and NIST 800-53.
- Ability to use judgment, initiative, and resourcefulness in deviating from established methods to modify, adapt, and or refine broader guidelines to resolve specific complex problems; research trends and patterns; develop new methods and criteria; and or propose new policies and practices.
- Plan, manage and provide guidance pertaining to IT Security architecture to include all phases of computer security (i.e., hardware, software, and telecommunications equipment, installation and evaluation). Work frequently requires the candidate to be involved in diverse projects simultaneously, several of which may have equally high priority.
- The work requires exceptional coordination and integration of Judiciary Information Security Framework (JISF) compliance activities, which requires its own body of knowledge. Decisions and actions taken by candidate will have a direct and substantial impact on services rendered.
- Excellent oral and written communications skills. Interaction and information gathering with coworkers and customers.

EDUCATAION/CERTIFICATIONS:

- Bachelor’s degree required, master’s degree preferred

- Industry leading certifications relating to IT security (CISSP, GIAC, etc.).

Send Resume to info@intellectualpoint.com job.