pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Mid-Level Policy Analyst

Overview	The position supports the Department of State, Diplomatic Security, Directorate of Cyber and Technology Security. The Policy and Standards Program is responsible for developing, promulgating, and maintaining Department cybersecurity policies and standards; developing and providing guidance on the Overseas Security Policy Board (OSPB) information systems security policy and standards; and providing guidance on existing policies and standards for the Department. The Program is also responsible for Department representation and coordination of National level policies and guidance. The Program handles exception requests for standards and policies within the Directorate of Cyber and Technology Security's scope of authority. Additionally, the program responds to user questions and inquiries about policy received via cables, memos, emails and phone calls.
Responsibilities	• Research, recommend, develop, maintain, and update domestic and overseas cybersecurity policies, to include use of new and emerging technology (e.g. WiFi, cloud, mobile devices), software, hardware, and other IT-related systems (e.g. VoIP, Building Automation Systems). • Lead efforts for updating DoS and Overseas Security Policy Board (OSPB) cybersecurity policies to address cloud technology adoption • Examine incoming requests for exceptions to policy and draft recommended decision memorandum to include requisite mitigation strategies • Coordinate clearances of all draft cybersecurity policies and memorandum with DoS stakeholders • Participate in intra-agency policy working groups (e.g. WiFi) and provide cybersecurity policy subject matter expertise • Provide support for the review and coordination for National level classified and unclassified cyber and communications security policies and guidelines • Respond to cables, memos, emails and phone inquiries regarding security policies and standards • Help maintain the contents of the Frequently Asked Questions (FAQ) web page and web portal website • Maintain databases for tracking incoming and outgoing policy documents, policy inquiries, exception requests • Provide status reports as required. Prepare contract deliverables to include Trend Analysis reports, Quarterly Status Reports, etc.
Position Description (HRTMS) – Qualifications	• Bachelor's degree in IT or related field with 5+ years of work experience or MA in the same fields combined with 3+ years of work experience • Experience in researching, developing, writing, and editing cybersecurity policies, best practices, standards, processes and procedures • Experience in research and analysis of information system issues and trends, and research and development in a technical discipline/field • Knowledge of, and experience drafting policy for, new technology, specifically cloud computing environments, cloud adoption, data classification, • Excellent written and verbal communication skills; strong organizational skills; research, analysis, and writing skills • Strong customer service and interpersonal skills to effectively relate to agency and customer needs; ability to build working relationships with leaders and key stakeholders • Proficiency with Microsoft Office • Some experience with the creation of IT security requirements, technical security safeguards, countermeasures, risk management, contingency planning, and data communications networking

	• Ability to work independently and as part of a team; ability to take initiative with minimal direction and to solve problems • Knowledge of, and experience with, current Federal security standards (e.g., FISMA/NIST, DOD, and CNSS) and cloud security standards • Familiarity with the Department of State's mission is preferred and work with global policies is preferred • CISSP and cloud certification (e.g. AWS, CCSP), are preferred
Preferred Qualifications	• Familiarity with the Department of State's mission is preferred and work with global policies is preferred • Security certifications such as ISC2: CCSP, CAP, SSCP, or CompTIA certifications such as: Security+ or CySA preferred. • CISSP is preferred