Perspecta

Title: Security Compliance Analyst

Location: Stennis Space Center in Hancock, MS

POC: Jennifer Jamison
Jennifer.Jamison@perspecta.com

Description:

- Participate in all steps of the Security Authorization and Assessment process for FISMA systems.
- Deliver all required documentation using the current DHS approved templates, forms, regulations, and methods.
- Continuously update all documentation as required.
- Provide advisement to stakeholders to assign resources and establish timelines to ensure the successful Security Authorization of a system.
- Review and validate all relevant NIST 800-53 and DHS 4300B Security Controls and/or applicable departmental policies for each IT system assigned.
- Ensure software installed in the production environment is evaluated and provide guidance regarding the potential for the software to introduce risk into the environment.
- Perform oversight of compliance with Vulnerability Alerts.
- Review and validate Plan of Actions & Milestones (POA&Ms) for each non-compliant control for each managed IT System prior to authorizing closure. Proper documentation to support the POA&M lifecycle shall be filed and updated as required, including well documented waivers and exceptions detailing the potential risk to the Authorizing Official.
- Perform in depth reviews of logs and other artifacts for each IT system.
- Provide, track and report security requirements throughout the project life cycle of all projects that are within the accreditation boundary of assigned systems.
- Provide timely and detailed responses to all data calls.
- Provide oversight and guidance regarding requests to modify technical policies such as firewall rules, ports, protocols, etc. for each IT system.
- Coordinate with and brief Federal staff on all activities pertaining to each IT system as requested.
- Continuously maintain a thorough understanding of all configurations, architecture, installed software, accounts (both Operating System and Application), data flows, ports, protocols, and other relevant data for each IT System.
- Coordinate with the appropriate operational group to accurately update the System Design Document for each IT system to reflect the approved state of each IT system.
- Participate in numerous working groups to provide training and guidance to numerous Components.
- Work closely with Office of the Chief Information Security Officer (CISO) to provide guidance and oversight for all requested initiatives.
- Associate’s Degree or 5 years of relevant experience.
- Must be able to perform all tasks identified in the Job Description.
- Knowledge of and experience with NIST SP 800-53, 800-53A, and 800-37.
- Experience with Risk Management Framework (RMF), POA&Ms, Security Authorization and Assessments, Vulnerability Assessments, FISMA Requirements, Waivers, Ongoing Authorization, Authority to Operate, Continuous Monitoring.

- Technical background and ability to review complex configurations for validation (i.e. Software Engineering, Network Engineering, System Administrator, Database Administrator background).
- Ability to compose and comprehend policy, procedure, guidance, demos, and training documentation.
- Expected to have superior communication and customer service skills to support training, help desk ticket responses, and support of a large customer base.
- Strong writing skills are required.
- U.S. Citizenship required.
- Must be able to pass a Federal background investigation.

Desired:

- Experience with Nessus, McAfee, Symantec, Retina, and Splunk software and output formats.
- Knowledge of DHS 4300B.
- CISA or CAP preferred – include certification # on resume.