

Cyber Security Engineer Cyber Security Engineer Cyber Security Engineer - Jacobs Diligent, result-driven and analytical IT security professional with 6+ years of extensive experience in conducting IT security assessment and compliance, system controls, system verification and validation testing techniques. Comprehensive knowledge on regulatory compliance for implementing and communicating Federal Information Security Modernization Act (FISMA) compliance for the Federal government as well as several internationally recognized commercial frameworks. Areas of expertise include NIST RMF, ISO and FedRamp. Cognizant of various industry standards pertaining to Federal and Commercial industries, resourceful, detail-oriented, and client focused, with a continuing passion for growth. Work Experience Cyber Security Engineer Jacobs March 2019 to Present Working in support of the United States Army Communications-Electronics Command under the purview of the Software Engineering Center, my current roles and responsibilities include:

- ? Performing information assurance (IA) policy development, implementation, and oversight for the SEC in support of the Army systems software sustainment mission.
- ? Providing guidance on integrating security and risk management activities into ongoing Software Life Cycle Management activities.
- ? Assisting with Accreditation and Certification activities to support the organizational transition from DIACAP to RMF.
- ? Creating SOPs and SEC regulatory policies IAW NIST SP 800-53A, FIPS 199 and other DODI and DODM documentation to identify weaknesses, conduct risks assessments and recommend and implement corrective actions as part of SEC.
- ? Conducting continuous monitoring activities to include annual assessments, POA&M, and utilizing the eMASS automated tool.

Jacobs Contract Avenue Technologies July 2018 to March 2019 Cyber Security Analyst

- ? Conduct security control assessments for new client systems based on NIST SP 800-53A Rev4 and in accordance with client policies and procedures.
- ? Assess an average of 4 projects a year using NIST 800 Risk Management Framework.
- ? Review systems categorization information utilizing FIPS 199 and NIST SP 800- 60 as a guide.
- ? Create Security Assessment Plan's (SAP) to document assessment schedules.
- ? Create and updated the following Security Assessment and Authorization (SA&A) artifacts: FIPS 199, SSP, RA, E-Authentication, ST&E, and Contingency Plan.
- ? Review and updated the Contingency Plan (CP) annually as part of the system security

documents, following NIST-800-34 Federal CP Guide. ? Review configuration management (CM) plans and procedures as part of security assessments. ? Responsible for tasks related to the system security Assessment and Authorization (A&A) and follow the Government IT security policies and standards. ? Utilize Risk Management Framework process to enable successful approval to operate (ATO). ? Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. ? Created and updated the following; Privacy Threshold Assessment (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Configuration Management Plan, Security Assessment Report (SAR) and Plan of Action and Milestones (POAMs). ? Work with stakeholders to ensure the identified weaknesses from vulnerability scans are remediated. ? Developed risk assessment reports to identify threats and vulnerabilities, also evaluates the likelihood of vulnerabilities being exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. IT Security Analyst IC Security Systems September 2014 to July 2018 Provided expertise in vulnerability management processes and network vulnerability scanning using Tenable Security Center. ? Responsible for the development of system security control test plan and in-depth security assessments of information systems. ? Developed security baseline controls and test plans used to assess implemented security controls. ? Conducted interviews, tested and examined organizational processes and policies for FISMA compliance. ? Assessed system design and security posture as well as advise information security compliance with FISMA and NIST SP 800-53 rev 4 controls. ? Created Security Assessment Reports (SAR) identifying the results of the assessment along with Plan of Action and Milestones (POA&Ms). ? Performed and recommended maintenance and system configuration settings in order to protect systems from emerging cyber threats. ? Participated in CDM meetings to discuss vulnerabilities and potential remediation actions with system and application owners. ? Developed System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements. ? Conducted follow up meetings to assist ISSOs and System Owners to close POA&M items. ? Assisted subscribers with vulnerability remediation, as necessary

? Conducted trending and analysis of monthly results to identify high risk vulnerabilities impacting the network and ensure proper security posture from a vulnerability management standpoint. ? Documented findings and severity levels of non-compliance in formalized reporting, written and oral briefs, etc. IT Security Specialist Deloitte Consulting - Rosslyn, VA May 2013 to September 2014 Conducted assessments of Federal client systems using NIST RMF Special Publication guidelines. ? Conducted IT risk assessments to identify system risk, vulnerability and threats. ? Assessed system design and security posture as well as advising stakeholders on information security compliance consistent with FISMA and NIST SP 800-53 control requirements. ? Conducted meetings with the client to discuss client's material weaknesses identified in an audit to gain an understanding and develop mitigation strategies for the findings. ? Provided mitigation strategies and recommendations to key stakeholders to enhance their security posture. Education Bachelor of Science Bowie State University - Bowie, MD Skills Cyber Security, Nist, Information Security, It Security, Microsoft

Name: Wanda Long MD

Email: ireyes@example.net

Phone: (808)719-1018x913