IT Cyber Security Engineer IT Cyber Security Engineer IT Cyber Security Engineer - RR Donnelley & Sons Spring, TX Work Experience IT Cyber Security Engineer RR Donnelley & Sons - Houston, TX April 2019 to Present Contribute to the development of information security policies, standards and procedures. Assist operations and development teams in aligning operating procedures with information security best practices Participate and captain security Incident Response processes. Apply internal controls and security concepts in a wide variety of information technology processes and appropriately assess the exposures resulting from ineffective or missing controls. Participate enterprise vulnerability management program and associated operational processes. Coordinate with development teams around security best practices, application vulnerability scanning and data privacy processes. Serve as internal information security consultant to business, development, and infrastructure teams, advising internal business units with current information about best practices, changes to the threat landscape and security related issues. Provide direct training to all employees, contractors, alliances, and other third parties, ensure proper information access in accordance with established organizational information security policies and procedures Security Analyst Exela Technologies - Woodland, TX January 2016 to March 2019 Conducts systems risk assessment through risk analysis, assesses assets within system boundaries, and identifies all possible vulnerabilities within systems. Assess security controls in accordance with the assessment procedures defined in the Security Assessment Plan (SAP) through examination, interviews, and testing. Conducts initial remediation actions on security controls based on the findings and recommendations of the Security Assessment Report (SAR) and re-assesses remediated control(s), as appropriate. Conducts security assessments by reviewing System Security Plans (SSP) to create Kick-Off Presentation Slides, Security Assessment Plans (SAP), and Security Control Assessment (SCA) matrices Uploads Plan of Action and Milestones (POA&Ms) into CSAM and validate artifacts provided to remediate POA&Ms. Drafts Security Assessment Reports (SAR) to provide stakeholders information regarding the security posture of their systems in accordance to the controls outlined in NIST SP 800-53 Rev. 4. Conducts meetings with various system teams to gather evidence, develop test plans, testing procedures and documents test results

and exceptions. Reviews POA&Ms and enforces timely remediation of audit issues. Reviews and updates System Security Plans (SSPs), Security Assessment Plans (SAP), Continuity of Operations Plans (COOP), Incident Response Plans (IRPs), and Information System Contingency Plans (ISCP). Provides support for documentation initiatives as related to System Security Plans (SSPs), Security Assessment Plans (SAP), Continuity of Operations Plans (COOP), Incident Response Plans (IRPs), and Information System Contingency Plans (ISCP). Develops a variety of Assessment & Authorization deliverables including; System Security Plan (SSP), FIPS 199 Categorization, PIA, ST&E, SAP, DRP, IRP, ISCP, CMP. Manage existing security solutions, including Meraki firewalls, anti-virus, and intrusion detection systems Implementation and management of security tools including Intrusion detection prevention tools Endpoint security tools (Symantec, Cylance) Vulnerability scanners (Nessus, Nexpose) Security Information and Event Management (SIEM) Splunk, SolarWinds Security Controls Assessor RR Donnelley & Sons - Columbus, OH April 2013 to December 2015 Ensured proper system categorization using NIST 800-60 and FIPS 199 Selected, and implemented appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. Developed System Security Plans (SSPs) to provide overview of federal information system requirements and describe the controls in place to meet these requirements. Reviewed and updated Plan of Action and Milestones (POA&Ms), in agency's Cyber Security Assessment and Management (CSAM) tool. Worked with system administrators to resolve POA&Ms, gathers artifacts and creates mitigation memos and corrective action plans to assist in the closure of POA&Ms. Guided System Owners and system teams through the ATO process, using NIST 800-37. Created, modified, and reviewed Incident Response Plans (IRPs), Security Assessment Report (SAR), Contingency Plan (CP) and POA&M for approval by the Authorization Official Performed security control assessment using NIST 800-53A guidance and as per continuous monitoring strategy requirements Developed a variety of Assessment & Authorization deliverables including; System Security Plan (SSP), FIPS 199 Categorization, PIA, ST&E, SAP, DRP, IRP, ISCP, CMP. Sets up POA&M ATO follow up pre-brief meetings with the System Owner, ISSO and other key stakeholders for each system with open

POA&Ms prior to the official follow-up briefs and as directed by the Client. Analyzed and updated System Security Plan (SSP), Risk Assessment Reports (RAR), Privacy Impact Assessment (PIA), System Security Test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M) Conducted Contingency Plan tests using the table top and/or functional method at least annually and updated the plan Devised plans to certify and accredit assigned Information system or information systems Ensured Configuration Management processes are followed to ensure that any changes do not introduce new security risks Education Associates in Applied Science in Applied Science Columbus State Community College - Columbus, OH May 2015

Name: Jessica Melton

Email: robertgilbert@example.net

Phone: 292-775-3938