Contractor Contractor Contractor - Valiant Solutions Bowie, MD Information Assurance/Risk Management Analyst with over 15 years of experience that includes performing IT security audits, operational risk management, updating security policies to help maintain the confidentiality, integrity and availability of sensitive data. Authorized to work in the US for any employer Work Experience Contractor Valiant Solutions - Washington, DC January 2018 to Present Information Security Continuous Monitoring Lead Perform security controls testing and reporting in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. Provide Authorization and Accreditation (A&A) support and assist in preparing authorization to operate (ATO) package. Enter and track plans of actions and milestones (POA&Ms) into Cyber Security Assessment and Management (CSAM) tool ensuring timely mitigation of vulnerabilities. Perform complex risk analyses which also include risk assessment. Establish and satisfy information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Support customers at the highest levels in the development and implementation of doctrine and policies. Perform analysis, design, and development of security features for system architectures. Monitor and analyze Cyber risk metrics to enable effective risk management and Information Systems Continuous Monitoring (ISCM). Risk Analyst IV Fannie Mae - Washington, DC April 2016 to December 2017 Liaise across relevant business, technology, and control functions to prioritize risks, challenge technology risk decisions, assumptions and tolerances, and drive appropriate risk response. Perform scenario analysis to determine level of impact if Personally Identifiable Information (PII) is leaked. Contribute to the establishment of metrics and tools to assess and report on inherent risks, control strength and residual risk in a consistent and objective manner. Assist with the development of remediation plans for technology deficiencies that address root cause and are sustainable. Monitor internal and external business, regulatory and technology environment to identify new or emerging risks. Collaborate with operational, technical, and corporate function personnel to foster a technology risk management culture that communicates a holistic risk profile of technology risk to Enterprise Risk Management (ERM) and various stakeholders. Monitor and analyze Cyber risk metrics to ensure first line of defense efficiency of risk controls. Senior Manager Kearney and Company - Alexandria, VA May 2015 to March 2016 Performed evaluation of the Corporation's information security program using the Federal Information Security Modernization Act of 2014 (FISMA) guidelines and requirements. Identified, documented, and tested IT controls for the following security control areas: Identity and Access Management, Configuration Management, Security Management, Segregation of Duties, Incident Response, and Contingency Planning. Tested the information security policies, procedures, and practices of Federal agency information systems thereby ensuring the accuracy and effectiveness of information security controls that support federal operations and assets. Recommend the development and maintenance of minimum privacy controls required to protect personally identifiable information (PII) in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. Applied NIST guidance to highlight to client the advantages of managing risks at the organization, business and information systems level, thereby ensuring IT goals and strategies aligned with the Corporations mission and objectives. Recommended NIST guidance to help clients maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Provided an assessment of management's internal controls and prepared a notice of findings and recommendations (NFRs) to communicate findings to management. IT Security Engineer - Contractor NASA Goddard Space Flight Center - Greenbelt, MD April 2011 to April 2015 Conducted review of Systems Security Plan (SSP) and Contingency Plan (CP) to ensure Authorization and Accreditation (A&A) package was complete. Performed security review on configuration change requests (CCR) and recommended whether proposed changes met appropriate security requirements. Evaluated and tested business processes and controls against information assurance guidelines and regulations (NIST 800 Series, FISCAM, FISMA and OMB). Analyzed and addressed cyber threats and vulnerabilities pertaining to process control networks and Supervisory control and data acquisition (SCADA) systems Developed test plans for unit testing and acceptance testing. Entered and tracked plans of actions and milestones

(POA&Ms) into Cyber Security Assessment and Management (CSAM) tool for project risks. Conducted security awareness training for federal staff and contractors regarding safeguarding personally identifiable information (PII) and other agency assets. Senior IT Security Analyst - Contractor Department of Labor - Washington, DC March 2008 to March 2011 Security Policy, Compliance and Audit Lead Performed tests of internal controls over financial systems and developed corrective action plans for identified control weaknesses in conformance with FISCAM and OMB Circular A-123, Management's Responsibility for Internal Controls. Documented business and systems processes to include key controls over financial reporting and systems operations. Developed, updated and maintained efficient agency-wide policies and procedures to ensure IT practices are compliant with government and security requirements. Provided Authorization and Accreditation (A&A) support and assisted in preparing authorization to operate (ATO) package. Provided IT support in the planning and execution of Federal Information Security Management Act (FISMA) assessments, Financial Information Systems Control Audit Manual (FISCAM) and A-123 audits by evaluating and testing business processes and controls in accordance with regulations (NIST 800 Series, and OMB). Entered and tracked plans of actions and milestones (POA&Ms) into Cyber Security Assessment and Management (CSAM) tool ensuring timely mitigation of vulnerabilities. Performed Security Self Assessments (SSA) for General Support Systems (GSS). Responded to incidents involving inappropriate use of IT resources and PII breaches. Implemented and tested product compliance with security technical implementation guides (STIGs) to verify compliance to a baseline level of security Ensured compliance and developed training packages for federal staff and contractors regarding safeguarding personally identifiable information (PII) and other agency assets. Contractor Food & Drug Administration - Rockville, MD October 2007 to February 2008 Junior IT Security Analyst Developed, updated and maintained efficient agency-wide policies and procedures to ensure IT practices are compliant with government and security requirements. Evaluated and tested business processes and controls against information assurance guidelines and regulations (FISMA, NIST 800 Series, and OMB). Supported IT Security Staff in Certification and Accreditation (C&A) efforts, to include the following:

IT systems assessment and documentation, security plan development, contingency plan creation, contingency plan testing and risk assessments. Performed Security Controls Testing and Evaluation (SCT&E), security training, policy creation and systems review. Assisted in identifying risks and the creation of the Business Impact Analysis (BIA) and Privacy Impact Assessment (PIA) of IT systems IT Audit Associate II Grant Thornton, LLP - Baltimore, MD October 2006 to October 2007 Performed general computer and application control reviews by testing IT General and Application Controls to determine effectiveness of controls. Performed SOX 404 compliance audit services for internal and external audit clients on application and IT general control reviews. Evaluated and tested business processes and security controls against recommended standards and guidelines such as OMB and COBIT standards Assisted with the development and implementation of Business Recovery and Continuity Plans. Education M.S. in Telecommunications and Computers George Washington University 2004 B.S. in Systems and Computer Science Howard University 2003 Skills SECURITY, FISMA, NETWORK SECURITY, SDLC, RISK MANAGEMENT Certifications/Licenses Certified Information Systems Security Professional (CISSP) December 2010 Certified Information Systems Auditor (CISA) June 2006 Project Management Professional (PMP) September 2016

Name: Sarah Mitchell

Email: patrickcarson@example.com

Phone: 565-466-1541x0709