Cyber Security Assessment and Authorization Analyst Cyber Security Assessment and Authorization Analyst Cyber Security Assessment and Authorization Analyst Silver Spring, MD I have over 5 years of experience analyzing and mitigating risks for federal and commercial entities. My areas of expertise are: NIST Risk Management Framework (RMF), Information Assurance, System Monitoring, regulatory compliance and loss mitigation. My knowledge of industry standards and ability to meet milestone deadlines make me a valuable addition to any organization focused on staying on top of information security matters. CompTia Security+ certification, Master s degree in Financial Management and graduate certificate in Project Management. CONTROLS & FRAMEWORKS FISMA, FIPS, FedRAMP, SaaS, PaaS, IaaS, ISO 27001, ISO 27002, COSO/COBIT, PCI DSS, DIACAP, FISCAM, HIPAA and HITRUST, Confidentiality, Integrity, Availability, Access Control, Audit and Accountability, Certification and Accreditation, Application control, Compliance Testing, Vulnerability Scans, Project Management, Risk Assessment, Change Management, Configuration Management, Contingency Planning, Policies and Procedures, Implementation, Incident Response, Physical Security, Environmental Security, Network Security, System Security, Personnel Security, OMB Circular A-130 Appendix III, Security Information and Event Management (SIEM) systems, NIST 800-53, NIST 800-30, NIST 800-37, NIST 800-34, NIST 800-53 and NIST 800-18 Work Experience Cyber Security Assessment and Authorization Analyst Generali Global Assistance (Contractor with MAA Associates) - Bethesda, MD October 2015 to Present Adhere to the NIST Risk Management Framework (RMF) to support the A&A process, including analyzing the development of supporting policies, procedures, and plans, designing and implementing security controls, testing and validating security controls, and analyzing and tracking corrective action plans. Analyze and update System Security Plans (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), Privacy Threshold Analysis (PTA), Contingency Plan and Contingency Plan Test, Security Assessment and Authorization (SA&A), Security Test and Evaluations (ST&E) and the Plan of Actions and Milestones (POA&M) Conduct security control assessments based on NIST SP 800-53A to identify system threats, vulnerabilities, and risks Conduct meetings to discuss vulnerabilities and potential remediation actions with system owners

Ensure identified weaknesses from vulnerabilities scans were remediated in accordance to the company s defined time frame Involved in the company s security awareness program to educate employees and managers on current threats and vulnerabilities Security Assessment Reports (SAR) are developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M). The reports evaluate the likelihood that vulnerabilities could be exploited, assess the impact associated with these threats and vulnerabilities and identified the overall risk level Prepare Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhered to NIST SP 800-53 standards Conduct follow up meetings to assist information system owners to close/remediate POA&M items Prepare recommendation reports that were made available to system owners to remediate identified vulnerabilities during the risk assessment process Support the annual security control assessment, by developing & gathering artifacts to ensure the system meets the Authority to Operate (ATO) FISMA compliance & reporting Information Security Analyst KPMG (Contract) - Baltimore, MD March 2014 to July 2015 Conducted kick off meetings with key officials and the audit team to determine the scope for the audit Assisted with collection of data, analysis of information and risk assessment Tested control self-assessments and review SSAE 16 to ensure the organization is in compliance with its defined system security policies Input corrective action plans into system. Followed up on corrective action plans and reviewed evidence for closure. Defined appropriate risk levels and corrective actions for issues identified Reported on assessment outcomes, risk level and associated recommendations Updated procedure documentation to incorporate process changes Implemented Sarbanes-Oxley Act (SOX 404) requirements, COSO, COBIT and PCI Security Standards Council (PCI SSC) where applicable Collected evidence via examination, interview and testing from various points of contact to update COSO, COBIT or PCI DSS finding report to test for effectiveness and adequacy of controls collected Regular monitoring of internal controls for any deficiencies. Deficient controls are then reported to the Business Owner for appropriate mitigation actions Conducted IT control risk assessments that include reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard (PCI DSS) IT Risk Analyst Accenture - Washington, DC April 2012 to February 2014 Analyzed data from multiple sources to identify discrepancies, spot fraud, and eliminate suspicion Interviewed and elicited information from team and clients to resolve issues Wrote reports, and documented evidence, findings, and recommendations Generated suspicious activity reports and risk management reports for supervisors and managers Determined existing fraud trends and assisted in the prevention of future trends Provided analyses where needed to determine inefficiencies within the department and implemented the fixes to these problems Assisted in coaching new hires, resolution specialists and identity theft coordinators as needed to effectively implement the processes to provide effective resolutions services Identified improvement opportunities and provided recommendations to management to modify id theft resolution techniques without negatively affecting client and customers experience Participated in system testing, validation and client notifications as needed and worked with sales and marketing teams, IT and other internal departments where necessary to resolve id theft issues Recognized as a problem solver and a person of high integrity with attention to detail IT Help Desk Support Europ Assistance USA - Bethesda, MD April 2011 to April 2012 Served as the first point of contact for customers seeking technical assistance over the phone or email Performed remote troubleshooting through diagnostic techniques and pertinent questions Determined the best solution based on the issue and details provided by customers Walked the customer through the problem-solving process Directed unresolved issues to the next level of support personnel Provided accurate information on IT products or services Recorded events and problems and their resolution in logs Followed-up and update customer status and information Passed on any feedback or suggestions by customers to the appropriate internal team Identified and suggested possible improvements on procedures Education Graduate Certificate in Project Management Boston University Graduate School of Management - Boston, MA December 2016 Master of Science in Management in Financial Management University of Maryland University College - Adelphi, MD December 2010 Bachelor of Science in Management in Business Management College de France - Paris, FR

August 2006 CompTia Security + Skills Jira (3 years), Microsoft office (10+ years), Microsoft outlook (10+ years), Ms office (Less than 1 year), Outlook (Less than 1 year), Rsa (3 years), Sap (Less than 1 year), Selenium (2 years), Selenium webdriver (Less than 1 year), Spss (2 years), Financial Analysis, Microsoft Excel, Sales, PowerPoint, Typing, Quickbooks, Marketing, Information Security, Nist, Siem, Cyber Security, Network Security, Comptia, Cybersecurity, It Security, Information Assurance, Splunk, NESSUS Certifications/Licenses Graduate certificate in Project Management Present Certified Identity Theft Risk Management Specialist (CITRMS) Present Certified Identity Protection Advisor Present CompTIA Security+ Additional Information ISACA Certified Information Systems Auditor (CISA) (expected July 2019) Certified Information System Security Professional (CISSP) (expected January 2020)

Name: Isaac Campbell

Email: williamsjohn@example.org

Phone: +1-695-359-3431x9768