Sr. Security Assessor Sr. Security Assessor Seasoned Information Security (SME) Professional Elkridge, MD Dear Hiring Manager: I am a competent Information Technology IT Security Professional (SME in Cybersecurity) and a trainer, and leader in various disciplines within the cyber realm, with over 15+ years in Information Assurance with over. I am a motivated self-starter, capable of working on the fly with regards to complex task and diverse initiatives. Professionally, I am extremely savvy both technical minded and regulatory minded. Any project or task presented to me will be thoroughly vetted and analyzed to present a finished product or solution to completion. I am detailed oriented and methodically effective in my approach. I work in all types of environments (i.e. classified and unclassified, face-to-face, team environments, and unassisted). I meet deadlines or precede timeframes to reach an appropriate and relevant solution, mitigation or plan. Very current and highly knowledgeable about advancements in new technologies, technologies, cyber subject matter, and issues plaguing the IT industry. Strengths: Industry Best Practices and Methodologies, Information Assurance/ IT Compliance, FedRAMP, IT Policies, and Building Strong Security Programs from the ground-up. Hobbies: Playing the Guitar Spending Time with My family Visiting National Museums Fitness Singing Trying Vegan Experiences World Travel Thank you for your time and consideration. I hope to have the opportunity to discuss the opening with you in person. V/r, Duane Cypress, MSCS; CISM; Security+CE Authorized to work in the US for any employer Work Experience Sr. Security Assessor Take2 Consulting - Vienna, VA July 2019 to Present 40hrs/wk. Monitors, analyzes, detects, and responds to cyber events and incidents. Supports dynamic cyber defense and delivers operational effects such as intrusion detection and prevention, situational awareness and data spillage. Maintains a secure cyber environment through configuration management, administration, and response actions. Analyzes network defense systems, such as IDS/IPS, SIEM and firewalls. May provide work leadership for lower level employees. Conduct technical security evaluations to identify security weaknesses resulting from vulnerability scans and security documentation reviews. Analyze results, identify false positives, and research mitigation solutions. Develop validation analysis documentation, including vulnerability management reports. Upload associated artifacts to the RSA Archer eGRC system. Conduct

Security Impact Analysis (SIA) for significant changes and review product and software release notes. Research various vulnerability databases, including the National Vulnerability Database, Security Tracker, TechNet, Flexracommunity, and CISecurity to identify known vulnerabilities in the products. Sr. Manager, Cyber/FISMA and Compliance ICF December 2016 to February 2019 40hrs/wk. Provided support for a ground up build and revamping the clients Federal Information Systems Modernization Act (FISMA) of 2014, regarding compliance to address gaps in federal requirements and mandates based on the Office of Management and Budget (OMB). Consulted with the federal client to identify IT investments and budget allocation in accordance with the Federal Information Technology Acquisition and Resource Act (FITARA) and the Risk Management Framework (RMF) NIST SP 800-37, 39 and 137 for the enterprise. Developed policies, guidance, frameworks, and standard operating procedures to ensure that administrative controls in accordance to the NIST SP 800-53 Rev. 4 are implemented properly. Conducted reviews of systems categorizations, assessing security controls, and monitoring vulnerabilities that may pose a risk and impact to the organization. The identification, mitigation of the identified residual risk is reported up to the client for a risk-based decision (RBD) and course of action. Managed personnel on project task for deliverables based on the statement of work for smaller supporting sub-agencies within the Department of Energy. Conducted, scheduled, and attended face-to-face meetings to address, plan, and identify both strategic and tactical business alignment from the organizational level up through the parent agency. Assisted in Business Development to address Cybersecurity for impending contracts. Cybersecurity, Information Assurance, and Policy Analyst III (Senior Consultant) Blue Glacier Management Group, Inc October 2016 to December 2016 October 2016 - December 2016 Title: Cybersecurity, Information Assurance, and Policy Analyst III (Senior Consultant) 40hrs/wk. Provided overarching support for IT policy and governance activities for the federal client. Worked in a team environment as a SME and refined the client's comprehensive risk management framework enabling cybersecurity management to make accurate risk-based decisions (RBD). Analyzed risk at the strategic level for the overall program, developed risk posture based upon the Risk Management Framework (RMF) in accordance with National Institute of Standards

and Technology Special Publication (NIST SP) 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle, thus implementing a comprehensive formal approach for the enterprise/organizational level or top tier rather than at an information system level or bottom tier. Implemented and maintained the Cybersecurity Risk Management Approach as defined by both NIST and the Committee on National Security Systems (CNSS) 1253. Reviewed and maintained the Cybersecurity risk plans of all client locations, as well as, analyzing documentation for assessment visits to include risk assessments and security controls in alignment with the NIST SP 800-53 Rev.4 and 800-53A Rev.4 for systems or series of systems. Developed Security Impact Analysis (SIAs)/Risk Assessment Reports to gauge the risk and impact of identified systems and General Support Systems (GSS). Introduced current event knowledge of legislation, initiatives, programs and cyber industry research for impact to supporting agency. Consulted the organization's Enterprise Cyber Security Advisory Board (ECSAB), specifically providing guidance on risk management and mitigation strategies for threats, risk and impacts. Managed and supported FISMA reportable systems in alignment with OMB A-130. Mapped risk with the categorization of systems in accordance to the highwater mark defined by the Federal Information Processing Standards (FIPS) 199, 200 and NIST SP 800-60 to the NIST SP 800-53 Rev. 4 security controls. Cybersecurity Information Assurance and Risk Management Specialist (Senior Consultant) InfoReliance Corporation January 2015 to October 2016 40hrs/wk. Provided overarching support for IT policy and governance activities for the federal client. Worked in a team environment as a SME and refined the client's comprehensive risk management framework enabling cybersecurity management to make accurate risk-based decisions (RBD). Analyzed risk at the strategic level for the overall program, developed risk posture based upon the Risk Management Framework (RMF) in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle, thus implementing a comprehensive formal approach for the enterprise/organizational level or top tier rather than at an information system level or bottom tier. Implemented and maintained the Cybersecurity Risk Management Approach as defined by both

NIST and the Committee on National Security Systems (CNSS) 1253. Reviewed and maintained the Cybersecurity risk plans of all client locations, as well as, analyzing documentation for assessment visits to include risk assessments and security controls in alignment with the NIST SP 800-53 Rev.4 and 800-53A Rev.4 for systems or series of systems. Developed Security Impact Analysis (SIAs)/Risk Assessment Reports to gauge the risk and impact of identified systems and General Support Systems (GSS). Introduced current event knowledge of legislation, initiatives, programs and cyber industry research for impact to supporting agency. Consulted the organization's Enterprise Cyber Security Advisory Board (ECSAB), specifically providing guidance on risk management and mitigation strategies for threats, risks, and impacts. Managed and supported FISMA reportable systems in alignment with OMB A-130. Mapped risk with the categorization of systems in accordance to the highwater mark defined by the Federal Information Processing Standards (FIPS) 199, 200 and NIST SP 800-60 to the NIST SP 800-53 Rev. 4 security controls.

Management and Engineering Technologies International (METI, Inc. -Prime Contractor) U.S. Forest Service Natural Resource Management (NRM), and Business Operations Organization (based out of Corvallis, OR) Cybersecurity Program Specialist (remote/teleworker) 40hrs/wk National Institute of Standards and Technology Special Publications September 2013 to September 2014 Collectively built a Cybersecurity program to reflect the National Institute of Standards and Technology Special Publications (NIST SP) 800 series, OMB A-123, 130, also the Federal Information Processing Standard 199, 200 and 140-2 encryption standards. Reviewed and initiated the U.S. Government FEDRAMP guidelines to align to the 800- 53 Rev3 baselines for Cloud and Virtualization infrastructure technologies (IaaS and PaaS) in a Service-Oriented Architecture (SOA) to include third party hosting has been ensured in tandem with the USDA's NITC. Worked with stakeholders to implement and govern clear Cybersecurity Metrics to best reflect the standards of NIST SP 800-55 and applicable SANS Top 20 Critical Cybersecurity Controls. Helped to mitigate recurring Plan of Action and Milestones (POA&Ms) issues identified in previous Office of the Inspector General (OIG) audits for a network consisting of an estimated 11,000 users. Assisted in implementing a Security and Awareness education program to ensure the proper training and

knowledge base is provided to alert users of their security responsibilities based on roles and privileges are recorded annually. Works with Computer Incident Response Team (CIRT) to analyze and evaluate security incidents. Structured an Assessment and Education program to ensure all regulations were met and also ensured all implemented policies and procedures are assessed and compared to strong Cybersecurity baselines such as DISA STIG checklists. Advised the application development team on implementation of the Open Web Application Security Project (OWASP) top 10 for secure, sound and effective security architecture and application development. Developed a Gap Analysis to determine costs and justification for additional resources and other appliances/products needed in order for day-to-day operations to mitigate and remediate an effective Cybersecurity Program for maintenance within acceptable risk levels. Identified vulnerabilities, recommended corrective measures and ensures the adequacy of existing NIST 800-53 rev.3 Information Technology Security controls of critical infrastructure to include geospatial data. Educated business unit managers, IT development teams, and the basic NRM user base community about risks associated with security controls affecting the U.S. Forest Service Network. Collaborated with Project Managers (PMs) to determine the impact of various project options and made recommendations on the best course of action for solution while addressing U.S. Government Cybersecurity requirements as mandated. Senior Information Security Analyst/Project Manager Volt Workforce Solutions September 2012 to September 2013 sub to Social & Scientific Systems, Inc.), 40hrs/wk. Worked with the project teams to understand and address their regulatory needs to define, implement, and align with Federal Information Security Management Act (FISMA) controls. Lead and coordinated Security Assessment & Authorization (A&A former known as C&A) efforts, identifies standard language that leverages generalized National Institute of Standard and Technology (NIST) 800-53 rev3 and 800-53a rev1 controls. Assisted the ISO in the development and maturation processes for standing up a Security Program and strengthen the overall security posture of the organization. Incorporated and integrated IT security language into the creation and modifications of policies, templates, and enhancements for the proposal writing process when bidding on new contracts. (i.e., Request for Proposal RFPs). Lead various security project

activities to include, but not limited to policy development, A&A deliverable management, architectural design, execution and overall project management. Related regulatory standards and guidance implemented were as follows: Health Insurance Portability and Accountability Act (HIPAA), FISMA, NIST 800 Series, ISO 27001; 2; 5, Office of Management and Budget (OMB) OMB Circular A-130, and Federal Information Processing Standard (FIPS) 199 and 200. Project Manager Integrity Consulting Solutions, LLC September 2011 to May 2012 Information Assurance/Cybersecurity (SME) 40hrs/wk. Worked with information assurance policies, guidelines, and regulations (FISMA, NIST 800 Series, OMB Circular A-130, and FIPS 199 & 200, etc.). Initiated, scheduled and performed training, and auditing associated with the Certification and Accreditation Process (Self Assessments, ST&E, PIA and etc.). Worked with researching and recommending advanced technologies to protect and secure the network against advanced persistent threats (APTs). Supported a Federal Agency implementation build of FedRamp (NIST SP 137 & 145; PaaS, IaaS, and SaaS) and Cybersecurity policies and techniques; use Unix/Linux, Ubantu, and Windows. Scanned servers and networks for vulnerabilities, help remediate Plan of Action and Milestones (POA&M) and enter into Trusted Agent FISMA. Lead a build-out of Security Operations Center (SOC) and procedure enforcement. Lead the developing of a roadmap to aggressively implement application technologies to track anomalies, and trends (a defense in depth) approach to secure the enterprise and IT systems. Work with Independent Verification and Validation to close known POA&Ms. Senior Information Security Administrator II/Risk and Compliance Chickasaw Nation Industries (CNI) September 2008 to September 2011 Food and Drug Administration (FDA), 40hrs/wk. Worked with Federal standards, regulations, and mandates and applied them to IT security policies in accordance with (HIPAA, SOX, FISMA, NIST 800 Series, OMB Circular A-130 and etc.). Initiate, schedule and perform training and auditing associated with the Certification and Accreditation Process (Self Assessments, ST&E, PIA and etc.) Supported the FDA Federal IT Security staff in Security Authorization and Assessment (SA&A), to include the following: IT systems assessment and documentation, security plan development, contingency plan creation, contingency plan testing and risk assessments. Essential Functions: Certification and Accreditation (C&A),

Security Testing and Evaluation (ST&E), security training, process review and audit, policy creation, customers' outreach and systems review. Coordinated with the Policy and Planning, Information Security Awareness (ISA), Computer Security Incident Response Team (CSIRT) and the Enterprise Architecture Team (EA). Run vulnerability scans in coordination with the Security Operations Center (SOC) using Tenable and Gideon - for compliance. Conducted FISMA related activities by way of with industry tools such as ProSight and Trusted Agent FISMA (TAF) to accomplish mission goals and objectives. Validated FISMA reportable risk annotated within the Plan of Action and Milestones (POA&Ms). Information Assurance Analyst FISMA, NIST July 2008 to September 2008 Food and Drug Administration (FDA), 40hrs/wk. Worked with Federal standards, guidelines, and regulations (FISMA, NIST 800 Series, OMB Circular A-130 and etc.) incorporating them into the information security program. Initiated, scheduled and performed training and auditing associated with the Certification and Accreditation Process (Self Assessments, ST&E, PIA and etc.) Supported the FDA IT Security Staff (in former C&A efforts) to include the following: IT systems assessment and documentation, security plan development, contingency plan creation, contingency plan testing and risk assessments. Essential Functions: Certification and Accreditation (C&A), Security Testing and Evaluation (ST&E), Security Training, Process review and audit, policy creation, customers' outreach and systems review. Information Security Consultant i - Secure, Inc February 2007 to June 2008 US Customs and Border Protection), 40hrs/wk. Lead various security components on multiple contracts. Facilitated, lead, and managed continuous evaluation of responsibilities for appropriate segregation of duties. Acted as the liaison between the technical leads, and the client to break down, and then explain system integrator access requirements. Performed various activities encompassing information security and information assurance (i.e. certification and accreditation, analysis, site visits, IT Security both enterprise and application , and Security Architecture) in support of the developing IT Security Program. Conducted Security Risk Assessments (SRAs') evaluating, testing systems (routers, switches, wireless access points, and open ports), enforcing, and implementing the following policies: NIST 800-53 Rev.2 & 800-53A, 47, 30, 26 and 18, FIPS 199, CBP 1400-05C, CBP 1400-02A, and Department of Homeland Security (DHS) 4300A. The

aforementioned policies, guidelines and standards were referenced for POA&M closure, remediation, mitigation and transference then entered into Trusted Agent FISMA (pilot) for various sites all over the world for US Customs and Border Protection and DHS. VTC Network System Administrator (Department of Defense L3 Communications January 2006 to February 2007 DOD ; Department of the Army), 40hrs/wk. Reviewed and applied the necessary security controls from the NIST 800-53, 30, 26, and DHS 4300A. Respond to telephone, electronic mail, and/or walk-in requests for support for all systems and equipment within the IMCEN HQDA Service Desk IT environment in accordance with current or revised Help Desk SOPs and/or service level agreements defined by the contingency plan. Troubleshot problems encountered using microcomputer software; Performed hardware/software testing and installation; Performed network and desktop based detection of viruses to counter/eliminate/control; Detect, contain and eliminate virus infestations; Responsible for being the primary point of contact for all conference room requirements including the set up, programming and maintenance of video and teleconferencing equipment. IT Specialist Tier I-II, 40hrs/wk Cherry Road Technologies March 2005 to January 2006 Assisted users with technical support and troubleshoot network problems for multi-systems. Track incident numbers and chat room monitoring. Troubleshoot international solutions for computer problems for our nation's finest military. Implemented active directory/ADEX (LDAPS, DNS, DHCP, domain controllers server , domains, trusts, GPOs, replication), Java, Novel, Outlook XP, Microsoft office suites, and working on a Tier I and II platform. SSGT Select U.S. Marine Corps. MALS 26 August 2000 to August 2004 6672-Aviation Supply Manager). 60 hrs/wk Assistant U.S. Marine Corps. MALS 26 2001 to 2003 Performed fixed and rotary wing unique applications and highly technical functions for the United States Marine Corp Aviation. Maintained the Database of fixed and rotary assets over $200 million. Managed, regulated, coordinated, and exercised control over avionic supplies, equipment, and other mechanized materials. Duties involved administrative and the Department of Defense specific procedures for the use of material handling equipment in the movement and storage of aviation unique supplies and equipment within military environments. Technical skills were required regarding military and commercial specifications on all supplies and equipment or services being

procured, stored, and maintained. These skills must be maintained in garrison, contingency and combat environments. Required to understand and apply operation of various state of the art multimedia, data scanning, and retrieval devices; office and warehouse management systems interface procedures; asset accounting functions; financial budgeting formulation; management and analysis; and the proper handling, storage, and disposal of hazardous material. Maintained aviation parts for type four series aircraft (confidential and Top-Secret briefings). Supervised between 20-30 personnel on a daily basis and provided scheduling, performance reviews, and counseling of staff. Other duties; conducted inventory on a monthly schedule, met deadlines for quarterly reports, devised a training system for instructional purposes, planned and scheduled training events, and defended my country during Operation Iraqi Freedom (OIF). Education Bachelor's in Computer Science Strayer University - Takoma Park, MD January 2005 to September 2008 Master of Science in Cybersecurity University of Maryland University College (UMUC) Skills Federal information security management act (10+ years), Fisma (10+ years), Information assurance (4 years), Nist (6 years), security (10+ years), Compliance, Regulatory Compliance, FDA, Information Security Military Service Branch: United States Marine Corps Rank: E-5 Certifications/Licenses CISM November 2018 to Present

Name: Edward Caldwell

Email: turnerstephanie@example.com

Phone: 001-287-906-6741