Independent IT Security Engineer Independent IT Security Engineer Independent IT Security Engineer - DXC Technology/Perspecta Atlanta, GA Proactive security-driven professional with expertise at managing IT Security products and services for DoD and Federal systems; and compiling deliverables required for Assessment & Accreditation (A&A) utilizing DOD and Federal Risk Management Framework (RMF) methodology; FISMA, FISCOM, and USCYBERCOM data feeds. An expert at driving NIST security assessment and control implementation using NIST 800-53A rev4 guidelines. A master at endpoint and network vulnerability management; reviewing enterprise vulnerability remediation and alerts; configuring vulnerability scanners; interpreting vulnerability threat feeds; and mitigating Host Based Security/Anti-Virus findings. Can perform operational tasks for Threat Log and Analysis; Software Firewall Settings, and Computer Network Defense (CND). In-depth experience on creating custom queries and dashboards; and analyzing vulnerability reports and trend analysis to reduce exploits using MS Access, SQL Reports, Tenable ACAS, MacAfee ePolicy Orchestrator, and various SIEM's and log analysis products. Holds Work Experience Independent IT Security Engineer DXC Technology/Perspecta - Washington, DC October 2018 to Present Utilized IA best-practices to reduce vulnerabilities for FDA patch management strategy; and documented results in monthly reports and patch remediation plans. Executed risk remediation for vulnerability testing, patch management, and Secure Configuration Management (SCM); efforts supported FDA to reduce 150, 000 exploits. Developed focused area patch management reports and analysis for 10 remediation teams; efforts resulted in a 35% reduction in enterprise vulnerabilities. Created process to analyze 14 QCD scans that contributed to 25,0000 credential failures; used MS Access to aggregate data and reference pass or fail checks. Developed high-level remediation plan to remediate over 350,000 Oracle Java vulnerabilities; designed and analyzed Plugins, IP Addresses, and subnets to plan deployment schedules. Follows NIST RMF to categorize, implement, and assess all security controls; created and managed ATO-related deliverables BIA, PTA, PIA, SSP, ITCP, and POA&M. Performs SA&A support services, including conducting independent control assessments, development of required security documentation, and the preparation, review, and briefing of completed authorization

packages. Developed vulnerability remediation documentation to cover data analytics, monthly reporting, and report delivery standards for executive teams. Assessed Unix, Windows, Red Hat, Oracle, and Third-Party applications for risk treatment and remediation action items. Independent Information Assurance Engineer GovernmentCIO - Atlanta, GA January 2018 to October 2018 Developed, updates and provide policy training as needed on the information systems security documentation templates (e.g. System Boundary development, System Security Plan (SSP), Contingency Plan, Contingency Plan Test, Business Impact Analysis, FIPS-199, authentication, Privacy Threshold Analysis, etc.) for VA's VistA Audit Remediation Program. Serves as the SME at developing and promulgating Security Assessment Plans, interpreting and evaluating implementations of FEDRAMP security controls; and analysis of risk assessment requirements, security architecture design, audit tools, and compliance for VistA Audit Solution. Executed full Security Assessment and delivered supporting documentation within aggressive timelines based on VA 6500, FEDRAMP, HIPAA, FISCAM, OMB 130 policies. Supports the Assessment and Authorization (A&A) Risk Management Framework process for all managed systems, networks, and enclaves (all security domains); ensure validity and accuracy review of all associated documentation. Work in coordination with both VAEC internal and external systems administrators, configuration management, and network engineers to ensure proper configuration and adherence to security standards regarding deployment actions. Serve as Security Controls Assessors for formal Security Test and Evaluation, Conduct of Security Certifications of VAEC systems/networks/sites assessing security control compliance; providing guidance regarding remediation and mitigation of identified vulnerabilities for VistA Audit solution. Independent Information Assurance Analyst Technatomy Corporation - Atlanta, GA November 2015 to January 2018 Analyzed and remediated vulnerabilities on DLA applications and systems for Risk Assessment Reports (RAR?s) and Federal Risk and Authorization Program (FedRAMP) via the execution of Fortify, ACAS, STIG Viewer, Vulnerator, and eMASS tasks. Provided risk management, security assessments, and ongoing authorization; and compliance support for RMF and DISA TaskOrds. authorization of DLA applications utilizing the Risk Management Framework

(RMF) and automated Security Assessment and Authorization tools. Performed FIPS 199 Control Baseline requirements to determine impact level and control categories for applications; and guided DLA J62GA on tailoring controls for DISA Cloud migration. Support the Plan of Action and Milestone (POA&M) identification, tracking, remediation, closure, and reporting process during SCA?s and SA&A. Review ACAS Scans and drafted remediation plans; and analyzed report findings to mitigate Java, .NET, RHEL, MS OS?s, and 3rd Party Application findings. Executed ACAS Scans, created repositories, managed report queries, and developed dashboards to reflect trend analysis based on USCYBERCOM Orders. Analyzed and prioritized vulnerabilities and provided remediation advice based on industry- standard classification schemes (CVE, CVSS, CPE). Used HP Fortify Static Code Analyzer (SCA) to conduct software and application vulnerability assessments; and served as the SME in scanning, vulnerability testing of networks, applications, databases, and operating systems. Information Assurance Analyst ASM Research - Atlanta, GA July 2014 to November 2015 Directed a team of 20 security experts to analyze NESSUS scan reports and assess validation scans for false positives and remediation strategies. Participates in Risk Exemption and Security Development initiatives; and develop requirements for File Share Remediation and risk treatment of open findings prior to SLA?s expiring. Developed Vulnerability Remediation workflow requirements for risk discovery, remediation, and exemption based on documented policies and procedures. Monitored data calls and suspense dates to remediate vulnerabilities, exemptions, and risks for Region 6 assets and applications; drafted Risk-Based decisions for legacy applications. Engineered technical solutions to mitigate vulnerabilities for 50,000 enterprise assets spanning 33 remote sites by focusing on VA?s Top 50 Critical Vulnerabilities, and infrastructure protection. Utilized Risk Vision GRC tool and VA OIG standards for agency-level comprehensive FISMA security assessment program, focusing towards continuous monitoring as prescribed in NIST 800-37 and 800-137; and VA?s Enterprise Architecture (VA EA). Information Assurance Analyst RLM Communications - Atlanta, GA October 2012 to July 2014 Administers technical advice, planning support for information assurance documentation required to support to maintain a key DoD forensic data center accreditation for the

US Army Forensic Science of Excellence (DFSoE) program. Integrates employee functional work requirements into a business framework to support Defense Forensic Science of Excellence (DFSoE) and STARLims availability; maintained cost scheduling and budget reports for project. Served as the principal architect to designing and implementing Change Control procedures to include: Change Workflow Process, Change Control Board documentation, and configuration management for Forensic networks. Led security assurance validation, artifact creation, vulnerability scans, assessments, remediation and IA implementation for desktop computers, servers, and databases. Manages assigned IA Controls, conducts risk assessments, documents compliance status of the validation results in the DIACAP Scorecard for ATO?s, and planned Security Test and Evaluations (ST&E) for Site Assisted Visits (SAV). Audited documentation required for SIP, DIP, C&A, and Plans of Actions and Milestones (POA&Ms) based on DIACAP procedures such as Business Continuity, INFOSEC Policies, and privacy based on DoD 8500 and NIST standards. Communicated with government CIO on existing security gaps and developed mitigation strategies based on DoD 8500, AR25-1, AR25-2, and FIPS for Site Assisted Visits (SAV). Researched procedures to integrate security products and services for forensic web-based applications and security. Information Assurance Engineer SOTERA Defense - Charleston, SC July 2011 to October 2012 Served as a subject matter expertise (SME) providing sustainment for IA to include C&A, CERT Readiness, IRM, ST&E, remediation, and POA&M for 135 enterprise servers using REM/Retina, McAfee ePO Orchestrator 4.5, IAVA?s, STIGs, vulnerability scans. Provided response to security requirements by performing security updates; utilize Server 2003 / Support Engineer HBSS - Charleston, SC March 2011 to July 2011 Served as a focal point to Concept of Operations (CONOPS) working group for establishing baseline operations, incident reporting, and contingency planning for HBSS. Configured applications for policy compliance and used reporting system to track, perform threat analysis, gather metrics, and mitigate risks based on CND task orders. Researched various threats and analyzed impacts for system changes and Information Operations Condition (INFOCON). Maintained theater architecture, management, and execution of all host-based IA and CND change controls, as part of CYBERCOM and JTF-GNO policies.

Processed improved HBSS software, hardware, and evaluation process by analyzing firewall logs, assessing security requirements, application settings, assets configuration, IPSIDS data, writing incident reports, briefing event details to leadership. Managed INFOCON for threats and coordinating remediation with network owners. Coordinating and conducting event collection, log management, event management, compliance automation, and identity monitoring activities using the MacAfee platforms Research, analyze and understand log sources utilized for the purpose of security monitoring, particularly security and networking devices. Develop, implement, and execute standard procedures for content management, change management, and lifecycle management for Log Management and SIEM products. Support day to day event parsing and repairing of events that have missing or incorrect information, create log source extensions, and flow management Performs all administration, management, configuration, testing, and integration tasks related to platforms to include content creation, maintenance, and administration tasks Creation of technically detailed reports on the status of the SIEM to include metrics on items such as number of logging sources; log collection rate, and server performance Administrator HBSS - Jacksonville, FL October 2009 to October 2010 Served as a focal point to Concept of Operations (CONOPS) working group for managing Host Intrusion Prevention System (HIPs), Policy Auditor (PA), McAfee Agent (MA), ePolicy Orchestrator (ePO), Asset Baseline Monitor (ABM), McAfee Anti-Virus (MA). Block unwanted programs such as spyware and adware within ePO repositories. Installed, repaired, and removed older Virus Scan versions and updated engine and dat files. Performed analysis via the ePO reports database on virus outbreaks and vulnerabilities to develop appropriate response for the incident. Worked with regional contacts to resolve technical issues. Performed system maintenance, and implemented, deployed and rolled out enhancements and new releases. Managed Group Policy (GPO's). Interfaced with upper management to relate the conditions of the structure and security on the network. Performed system monitoring as well as developed and maintained operational supports standardization and procedural SOPs for the McAfee ePO product. Senior Security Analyst SAIC - Jacksonville, FL April 2009 to August 2009 Provided technical assistance to System Engineering team on all matters including functional layout,

COOP operation, security integration, technical requirements, and C&A. Instituted a vulnerability management program to control threats and integrated security compliance for systems. Coordinated tasks and scheduling with security engineering team and outside customers Performed a quality check after conducting assessments to ensure 36 workstations was in IA compliance. Independently developed a variety of DIACAP deliverables including: System Security Plans, Security Design Documents, Vulnerability reports, Privacy Impact Assessments, Security Annual Assessments, and Contingency Plans. Enterprise Management 2008 to 2008 software, and expertise to advise clients on resolving compliance issues for over 40,000 assets. Troubleshot Server 2003/2008 software problems and applications; configured, tested, and installed new and/or enhanced software though registry modifications, and configuration changes. Engaged with technical experts from DISA and vendors to mitigate complex system vulnerabilities. Worked with various technical teams to address security configuration based on DISA?s Secure Tool Suite performed security checks and associated changes to maintain STIGcompliance. Utilized REM Enterprise Manager to gather trend analysis, statistics, and information for threats and risks associated with log data correlated from 27 Retina Scanners. Created and maintained baseline configuration for all centrally managed assets through SIEM feeds. Utilized Server 2003/2008, Retina Vulnerability Scanner; REM Security Management Console and technical expertise to advise IAM?s on resolving issues related to defensive security solutions. Education MS University of Maryland University College December 2010 BS University of Maryland University College May 2006 Skills Security, Hipaa, Nessus, Nist, Fisma, Cyber security, Sdlc, Remediation, Risk assessment, Risk assessments, Security engineering, Needs assessment, Best practices, Metrics, Internal controls Additional Information Skills Risk Assessment able to align resources, processes, and services for Risk Assessments and NIST Risk Management Framework (RMF), eMass, CSAM, Cyber Security Readiness Inspection (CCRI), Nessus, SCAP, & STIG scans. Expert at conducting Security Control Assessments (SCA) of threats and vulnerabilities to determine deviations from acceptable configurations, enterprise security standards, or local policies; and assessing the level of risk to determine appropriate countermeasures for sustaining FISMA compliance. Vulnerability

Management adept at developing security dashboards, vulnerability remediation process, and conducting enterprise vulnerability scans using Fortify and Assured Compliance Assessment Solution (ACAS). Holds senior level knowledge on developing metrics, trend analysis; reported anomalies, unapproved system configurations, detected vulnerabilities, remediation, and risk acceptance and reporting using HBSS, HP Fortify, Retina, NESSUS, or IBM Big Fix. Security Engineering possess a track record at improving needs assessment, information protection, and integrating security, applications, and assets via the SDLC. Utilizes various skillsets to identify security safeguards via NIST 800- 53, OWASP, SANS Top 25, HIPAA, and CNSS 1253 for security best practices and internal controls.

Name: Aaron Macias

Email: jjohnson@example.net

Phone: +1-929-323-1154