

Sr Information Systems Security Officer (ISSO) Sr Information Systems Security Officer (ISSO) Sr Information Systems Security Officer (ISSO) - Unisys Federal Systems Alexandria, VA Possesses over 16 years of experience supporting the Department of Defense (DoD) (Joint, Navy, Air Force, Army), Intelligence Community (IC), and Department of Homeland Security (DHS/Customs and Border Protection (CBP) in the Cyber Security field. Experience include Risk Management Framework (RMF), Certification and Accreditation (C&A), System Security Assessment, product and system analysis, process re-engineering, work flow analysis, requirements analysis, policy design and implementation, planning and migration of legacy computing environments. Experienced in hardware deployment and Department of Defense Information Assurance Vulnerability Alerts (IAVAs) compliance testing, downloading and set up of user's PKI, and system and policy documentation. Possesses a general knowledge and experience working with Windows operating systems and Unix/Linux environments, hardware, software implementation, and telecommunications technology. Proficient with Microsoft (MS) Office Suite (Word, Excel, PowerPoint) Experienced in product development and marketing. Possesses experience in project management, office management, development of training materials, and training delivery. Work Experience Sr Information Systems Security Officer (ISSO) Unisys Federal Systems - Alexandria, VA February 2019 to Present Unisys Federal Systems February 2019 - Present Position: Sr Information Systems Security Officer (ISSO) Client: Customs and Border Protection (CBP) (Alexandria, VA) Responsible for managing, developing, reviewing, maintaining, and implementing System Security Plans (SSPs), Continuity of Operations Plans (COOP), Plan of Action and Milestones (POA&Ms), creating and submitting Waivers and Risk Acceptances for system vulnerabilities. Conducted continuous monitoring and periodic self-inspections of computer systems to confirm security compliance utilizing NIST 800 series guidance, DHS, CBP and other policy directives. Tracked system security posture using the XACTA (IACS) tool. Proactively supported reporting of progress to management, and made recommendations for improvements as needed. Reviewed Nessus, Webinspect, and DBProtect security scans and provided reports and recommendations on vulnerability remediation. Reviewed DHS ISVM alerts for applicability to assigned systems and

collaborated with technical stakeholders on remediation efforts. Responsible for conducting annual Contingency Plan Testing (CPT) and annual Security assessments. Active contributor to system Penetration Testing. Supported development of management briefings on the security posture of assigned systems. Assisted directorate with security-related data call responses and/or audit responses. Reviewed and approved/denied system change requests. Supported periodic reviews (re-certifications) of Privileged user accounts (Developer, Admin, etc.). Active participant and contributor during annual KPMG audits. Acted as the primary interface between System Owners (SO), Business Owners, and Administrator teams. Information Systems Security Officer (ISSO) KForce - Reston, VA September 2018 to February 2019 VA) Ensured that system security requirements are addressed during all phases of the information system's lifecycle Developed and maintained security RMF documents, including SSPs, CONOPS, Test Plans, SCTMs and other system security documentation Conducted reviews and updated security documentation Support and cooperate with internal risk assessments and systems audits Authored/ coordinated the development of other required system security plans: Configuration management (CM), Contingency Plan (CP), Continuity of Operations (COOP), Disaster Recovery Plan (DR) and Incident Response Plan (IRP) Supported and executed continuous monitoring strategy for assigned systems. Conducted ongoing security assessments of security controls for (3) systems utilizing the Risk Management Framework (RMF), NIST-800-53, NIST 800-37, and DHS 4300A. Established review of system audit trails and ensured their review, reporting and remediation as needed Requested required information system vulnerability scans in accordance with established policy Developed system POA&Ms in response to reported vulnerabilities Ensured compliance with annual FISMA deliverables and reporting Ensured that assigned information systems are operated, maintained and disposed of in accordance with approved security policies and practices Participated in daily scrum meetings to ensure security is included in software development lifecycle. Worked closely with scrum masters to ensure all security deliverables are being met. Information Security Support Officer (ISSO) Alethix, LLC - Springfield, VA March 2018 to September 2018 VA) Responsible for managing, developing, reviewing,

maintaining, and implementing System Security Plans (SSPs), Continuity of Operations Plans (COOP), Plan of Action and Milestones (POA&Ms), creating and submitting Waivers and Risk Acceptances for system vulnerabilities. Responsible for conducting annual Contingency Plan Testing (CPT) and annual Security assessments. In charge of taking existing systems from Authority to Operate (ATO) to Ongoing Authorization (OA). Acted as the primary interface between System Owners (SO), Business Owners, and Administrator teams. Conducted ongoing security assessments of security controls for (3) systems utilizing the Risk Management Framework (RMF), NIST-800-53, NIST 800-37, and DHS 4300A. Coordinated and assisted in annual KPMG financial systems audit preparations. Responsible for mentoring junior Information System Support Officers.

Actively participated in successfully moving current systems into On-going authorization (OA). Tailored security controls assessment frequencies and updated expired controls. Tracked system security posture using the XACTA (IACS) tool. Participated in implementing Common Controls to be utilized by other systems. Reviewed system audit logs using manual and training to use automated tools (Splunk). Performed security impact analysis and provided approval recommendations. Performed regular account reviews in accordance with Department of Homeland Security (DHS) policy. Maintained system inventory lists. Analyzed monthly and ad-hoc vulnerability scans to track weaknesses as required. Reviewed and responded to ISVMs and ensured all required actions were addressed. Updated and maintained Plan of Action and Milestones (POA&Ms) for assigned systems. Actively worked with System Owners to address and mitigate POA&M findings. Collaborated with customers regarding the closure and / or transfer of POAMs. Reviewed and updated all required system documentation including but not limited to, the System Security Plan (SP) and Contingency Plan (CP). Coordinated and provided support during Contingency/Business Continuity plan tests. Reviewed, provided recommendations and approved proposed Change Requests (CR). Information Security Support Officer (ISSO) Crystal Management, LLC September 2016 to March 2018 Information Assurance Support Officer (IASO) Customs and Border Protection (CBP) - Springfield, VA January 2016 to September 2016 **Due to contract change, responsibilities are the same as listed in Alethix LLC. ** Chenega Corporation January

2016-September 2016 Position: Information Assurance Support Officer (IASO) Secure IT Operations Board Program Manager Castalia Systems, LLC - St. Louis, MO October 2015 to December 2015 MO) Coordinated and conducted weekly Portfolio/Project Review meetings. Coordinated and conducted Monthly Metrics Review meetings. Advised the individual project managers on developing, articulating, and presenting their projects. Compiled meeting summary notes and disseminated as appropriate. Coordinated and Participated in Monthly Metrics meetings. Actively participated in the annual Organizational Planning meeting. Coordinated and advised SharePoint developer to implement ongoing process improvements into the Board's Sharepoint site. Prepared agendas for Project Board meetings. Consulted and advised project managers on their respective project's progress. Conducted pre-board reviews and rehearsals with Project Managers as necessary Worked closely with PMs to align Project Portfolios to reflect leadership expectations. Developed the Project Board Standard Operating Procedures (SOP). Developed a Project Board Continuity Binder. Developed templates for Project Managers to utilize to standardize documentation formatting. Active member of program restructuring and realignment efforts. Security Controls Assessor (SCA) Castalia Systems, LLC - St. Louis, MO December 2014 to October 2015 MO) Performed comprehensive security assessments of systems using identified and applied security controls. Assessed systems for compliancy of security baselines and security controls based on operating system, network, and application of appropriate STIGS. Assisted with determining risk and prepare security assessment reports. Provided formal recommendations on security posture of systems assessed. Participated in group and organizational working groups and meetings as required. Provided testing support via approved test plans and tools. Provided support with authoring/co-authoring of documentation such as Standard Operating Procedures (SOPs) and System Security Test Plans using NIST and CNSS guidance with the ICD 503 Process. Participated in off-site FISMA compliance assessments and inspections. Information Assurance Support Officer (IASO) Advanced C4 Solutions October 2011 to September 2014 Client: US Army (Camp Humphreys/Sobingo Compound, S. Korea) Provided Certification and Accreditation (C&A) support accrediting systems and/or networks using the Department of Defense Information

Assurance C&A processes: (DIACAP), DODIIS, NIST 800-53, and ICD 503. Responsible for Continuity of Operations Plan (COOP) including maintenance of plans, procedures and automated call tree capabilities. Drafted and co-authored Brigade Standard Operating Procedures (SOPs). Assisted with integration of new capabilities with new and security systems. Acted as backup administrator for automated tools (HBSS and Retina) to support organizational cyber security and compliance program. Developed documentation including briefings, papers, reports, charts, and diagrams related to Information Assurance, C&A, processes and procedures. Provided the 501st MI BDE with effective project management support. Responsible for FISMA, POM and other compliance reporting as required. Served as an active member of the Information Assurance Team throughout a systems life cycle. Acted as the primary POC for the IAM in all C&A matters within the Brigade currently supporting INSCOM. Provided guidance and oversight to military personnel and other team members. Provided Trusted Agent (TA) support for PKI. Information Assurance Manager (IAM) BAE Systems January 2010 to October 2011 Client: US Airforce (Osan AB, S. Korea) Advised and supported all required security approvals regarding Certification and Accreditation (C&A) processes. Provided subject matter expert (SME) advisement on Certification and Accreditation (C&A) technical writing support in generating Systems Security Authorization Agreement (SSAA) using the DITSCAP and Certification and Accreditation packages in the DIACAP processes. Supported C&A approval processes for NIPRNET, SIPRNET, JWICS, and the Coalition network utilizing DoDD, AFI, DCID 6/3, and TEMPEST/EMSEC. Worked closely with the Configuration Manager and provided guidance on IA compliance issues regarding software and hardware. Utilized results obtained from security tools (Retina, VMS, Cross Domain Solution) to assess security posture of systems for certification and accreditation. Assisted in firewall audits and compliance audits. Provided support in security incident investigations and reporting. Worked closely with Intelligence Community in Certification and Accreditation efforts of DODIIS systems. Developed Standard Operating Procedures (SOP) on day-to-day operations. Served as a member of the Control and Configuration Control Board (CCB) and Engineering Working Group (EWG). Provided assistance with security incident reporting in collaboration with the Security

Manager. Provided guidance on preparation for compliance inspections. Provided SME advisement on process re-engineering of the Information Assurance department to government lead. Provided SME advisement on organization Continuity of Operations Plan (COOP) and Contingency Plan (CP) development. Provided SME advisement on personnel certification based on DoDD 8570.01-M. Recommended IA certification training plan and identified potential training opportunities. Associate Secure Systems Engineer BAE Systems - Honolulu, HI September 2005 to January 2010 HI) Assisted in evaluating the effectiveness of legacy systems. Collected and analyzed data to support requirements data. Provided solutions based on research and analysis to improve efficiency and effectiveness of existing security applications. Monitored and evaluated data using Symantec SPAM filtering application for SMTP and Tumbleweed. Prepared and maintained documentation in relation to secure systems. Reviewed and made recommendations for information assurance solutions based on knowledge of networks and existing application performance. Executed documentation in relation to the Federal Information Security Management Act of 2002 (FISMA) and assisted with the planning of Shipyard implementation and compliance. Acted as the FISMA liaison between the PHNSY& IMF, NAVSEA Headquarters, and the Department of Energy's Cybersecurity Division for reporting and FISMA compliance. Responsible for the development and implementation of the Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility (PHNSY & IMF) workforce certification (Policy Driver: DoDD 8570.01). Responsible for the execution of the Pearl Harbor Shipyard's annual \$200K training budget and compliance of the certification of all identified Shipyard personnel (Civil Service, Military and DoD Contractors) with emphasis on Information Assurance positions. Responsible for the identification of training resources and providing guidance on training plans and budget forecasting. Provided audit support in reviewing proxy logs for inappropriate government IT resources usage, departmental security surveillance and reporting, incident reporting, and investigations. Provided preliminary support to the Information Assurance Manager (IAM) in the research and initial documentation phase of the PHNSY & IMF's Continuity of Operations Plan (COOP). Provided Certification and Accreditation (C&A) support in writing Systems Security Authorization Agreement

(SSAA) using the DITSCAP processes and was formally trained to utilize the DIACAP processes.

Business/Data Analyst Referentia Systems - Honolulu, HI July 2005 to September 2005 Provided technical and administrative support to the Client Technical Support Representative to accomplish the J644 mission. Assisted in interfacing with vendor regarding billing and accountability of government-purchased Information Technology services. Maintained proprietary NET database of NMCI users, assets and applications as pertaining to Headquarters U.S. Pacific Command (HQUSPACOM). Supported the coordination of scheduling and planning of the migration of the legacy network to the new NMCI network. Expedited support for the transition, operations and sustainment of workstations in the new NMCI environment. Processed information technology requests on behalf of client. Acted as a liaison between Directorates and the J644. Functioned as a Trusted Agent working for the Camp Smith LRA. Coordinated and expedited PKI and X.509 (RASP) user requests. Assisted clients in the download set up of PKI certifications. Provided support in internal process improvement and streamlined existing inefficient processes. Trained and supervised Contractors and Reservists to use proprietary database and information request submission system. Assisted with business process re-engineering to streamline process flow of submission of IT requests. Responsible for process re-engineering and work flow analysis.

Business/Data Analyst Anteon Corporation - Honolulu, HI January 2004 to July 2005 Due to contract change, responsibilities are the same as listed in Anteon Corporation ** Education Master's Skills Word, Security Certifications/Licenses CompTIA Security+ CE Present AWS Certified Cloud Practitioner August 2019 to August 2022

Name: Kevin Carter

Email: brooksamanda@example.org

Phone: (707)448-4179x339