Information Systems Security Officer (ISSO) Information Systems Security Officer (ISSO) Information Systems Security Officer (ISSO) - Tech Flow Inc Fredericksburg, VA Work Experience Information Systems Security Officer (ISSO) Tech Flow Inc - Sterling, VA January 2018 to Present Primary Client: Defense Intelligence Agency; Development and Enhancement for Enterprise Applications (DEEA) Ensure that system security requirements are addressed during all phases of the information system's lifecycle. Develop and maintain security RMF documents, including SSPs, CONOPS, Test Plans, SCTMs and other system security documentation; Conducts reviews and updates security documentation, e.g. review and update IAW continuous monitoring and federally mandating auditing requirements. Support and cooperate with internal risk assessments and systems audits. Author and coordinate 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). Support and execute continuous monitoring strategy for assigned systems. This includes establishing system audit trails and ensuring their review, reporting and remediation as needed. Request required information system vulnerability scans in accordance to establish policy; Develop system POA&Ms in response to reported vulnerabilities. Ensure compliance with annual FISMA deliverables and reporting. Work in a scrum/agile environment Ensure that assigned information systems are operated, maintained and disposed of in accordance with approved security policies and practices. Information Systems Security Officer (ISSO), nLogic - Fort Lee, VA April 2016 to January 2018 Primary Client: Defense Commissary Agency (DECA); Telecommunications and Network Branch (LEITT) Provide trend and anomaly analysis, support to insider threat investigative activities and production of limited scope threat assessments to assist in mitigating identified personnel, physical, and information security vulnerabilities. Serve as a Cybersecurity expert for the program throughout all stages of acquisition, systems engineering, and maintenance processes. Prepare formal briefings and analytic products with reports of findings and recommendations upon which security countermeasures, investigations and remediation actions may be based. Utilize user activity monitoring, databases, data mining and visualization tools in order to discern threats and conduct

limited inquiry and testing to prove threat and risk hypotheses for further investigation and resolution. Compare cyber counterintelligence analytic results against known tactics, techniques and procedures employed by adversaries to exploit individuals and networks. Provide Cybersecurity Assessment and Authorization (A&A) services; support NITTF, CCRI, CNDSP, and PCI audits. Develop DoD Information Assurance Certification and Accreditation Process (DIACAP) and Risk Management Framework (RMF) packages. Remediate existing vulnerabilities or develop mitigations that minimize impact, likelihood, or risks, and work with the program to incorporate findings into the system POA&M. Developing proposed policies and Tactics, Techniques, and Procedures (TTP) in support of the Army's Defense-in-Depth strategy and the Department of Defense Global Information Grid (GIG) Vision. Ensure system designs and implementations are consistent with Department of Defense (DoD) and DON Cybersecurity policies, requirements, and directives. Implement agency wide security awareness training and suspicious activity reporting. Sr. Insider Threat Analyst ICF - Fort Lee, VA November 2014 to April 2016 Primary Client: Defense Contract Management Agency (DCMA); Information Assurance Directorate (IT-K) Under guidance of DOD/DISA serve as CNDSP - defined, planned, designed, and evaluated information security systems. Conducted ongoing Insider Threat activity analysis and prepare internal briefs and evidence cases of findings for management review and decision-making. Implemented training and awareness of IT security programs for all users Conducted analysis for indicators of Advanced Persistent Threat (APT). Performed vulnerability and cyber security assessments and gap analysis of security program and related systems and networks. Applied necessary controls. Conduct penetration tests against systems and networks. Applied digital forensic analysis, intrusion analysis, data recovery, malware analysis, and reverse engineering techniques for identifying and characterizing cyber threats. Develop and maintain tools, techniques, countermeasures, and trends related to data hiding, covert communications, encryption, network security, and offensive/defensive cyber operations. Assist in deterring, identifying, monitoring, investigating, and analyzing cyber intrusions. Prescribe cyber security best practices and anti-malware techniques to address weaknesses in cyber assets and combat sophisticated threats against those assets. IT

Forensics Analyst, Insight Global Chevron - Information Technology Company - San Ramon, CA November 2013 to November 2014 Primary Client: Chevron - Information Technology Company; IRSM Incident Management Forensics Reviewed and processed cases for senior investigators. Performed forensic investigations of IT assets through the utilization of accepted procedures to document alleged incidents of inappropriate use of corporate assets. Extracted digital data from any computer, server, database storage media, mobile device and guaranteeing its accuracy and reliability for a court of law, if necessary. Participated in Global Security and Law function authorized investigations; multiple interactions with human resources and attorneys. Experience in internal, HR, divestiture and eDiscovery cases. Performed investigative analysis by locating electronic artifacts and subsequently testifying to the methods and protocols involved; worked with LAW LFA- IT to get findings and load for review. Performed evidence handling, by labeling the evidence properly, packaging it and sealing it in order to meet the Federal Rules of Evidence and to fulfill the Forensics Operations Procedures. Maintained confidentiality of information received through interviews and all investigations and legal matters being addressed. Gained knowledge of agile work environment. Network Security Specialist II Jacobs Technology - Fort Lee, VA June 2012 to November 2013 Primary Client: Defense Information Systems Agency (DISA); Software Engineering Center (SEC-LEE); Tactical Logistics Directorate at Fort Lee Developed and implemented enterprise information assurance/ security standards and procedures following the DIACAP process. Gained experience in the interactions the various IAVAs may have with the STAMIS Support testing as necessary to ensure functionality following the installation of the patch and provide feedback to the ACERT for issues that may exist within the patches. Analyzed results and STIGS from Retina, SCAP, NESSUS or Gold Disk - Platinum level scans in order to make recommendations to System Manager (SM). Built and tested images of SEC-LEE programs: SAAS MOD, PBUSE, SAMS-E, FMTP, ULLS AE, SARSS-1. Experience with Ghostcast Server/Acronis and SCCM in image development/deployment. Established and satisfied information assurance and security requirements based on the analysis of user, policy, regulatory, and resource demands. Consult with vendors on findings. Performed analysis, design, and

development of security features for system architectures. Analyzed and defined security requirements for computer systems, which may include mainframes, workstations, and personal computers. Performed vulnerability/risk analyses of c omputer systems and applications during all phases of the system development life cycle. Developed, researched, and maintained proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption. Provided computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery. Performed assessment on cloud vendors using FedRamp Desktop Support II Logistics Management Resources - Fort Lee, VA November 2011 to June 2012 Primary Client: Army Logistics University at Fort Lee Assisted in the configuration, installation, commissioning, operation, and trouble-shooting of information technology hardware, software, operating systems and networking issues in support of the Army Logistics University (ALU) and Sustainment Center of Excellence (SCOE/CASCOM) schools. Assisted in the deployment of Windows 7; primary deployment led to an ALU wing (100+ users). Supported the workload of the student-user training stations, troubleshooting of wired and wireless networks, SIPRNET/NIPRNET, and other issues including: IAVA compliance, personnel account management, classroom system management, and information assurance conformity. Diagnosed and problem-solved for various incoming inquiries and requests, including: replacement of parts (i.e., modems, monitors, printers, memory chips, etc.), manage repair outsourcing, manage software or files modifications/configuration/replacement. Provided technical support to students that may have connectivity or issues operating Standard Army Management Information Systems (STAMIS),BCS3, CRXXI and ATSC Applications: Kanguru imaging systems, Track- It trouble ticket system, and Dame Ware/SCCM. Help Desk Analyst SAIC - Richmond, VA December 2009 to November 2011 Primary Client: Defense Logistics Agency Level 1 and Level 2 troubleshooter for technical, functional, hardware, and other peripheral issues in support of more than 10,000 users world-wide. Working familiarity of DOD and commercial applications and systems, including: SAP, DPACS, Oracle, Fusion, EBS, Red Stone, AMPS, CITRIX, CFOL, SIPRNET/NIPRNET, BES, SCCM

Provided ongoing analysis and support for ongoing Windows 7 deployment for local and global

users across several military and government installations. Processed, tracked, and managed open/closed work-order service tickets using Magic and Remedy. Supported the installation of new software/hardware configurations; test user systems as required. Performed basic networking maintenance functions such as user creation and assignment of rights and permission in Active Directory. Knowledge of remote access (SMS) and VPNs (JUNIPER). Administered file-backups, system restores, imaging, software installations. Consistently ranked #1 for Calls Taken and Trouble Tickets Opened/Closed; overall top 10%. Education MCITP Virginia Polytechnic Institute & State University Links https://www.linkedin.com/in/chris-clark-9725302

Name: Andrea Williams

Email: brownphilip@example.org

Phone: 001-346-755-6901x980