Cyber Security Analyst Cyber Security Analyst Vulnerability Analyst - CGI Federal Arlington, VA Work Experience Cyber Security Analyst January 2014 Present | SYSUSA / PEPCO - Washington, DC January 2014 to Present Responsibilities Supported the security assessment of SSN (Silver Spring Network) AMI (Advanced Meter Infrastructure) Software UIQ (Utility IQ) for PEPCO Holdings Inc. Smart Grid. Network architecture review of IT & OT network. Performed security baseline assessment of system enclave that included Server 2008 R2, Red Hat 6, Cisco, Infoblox, Oracle using manual and automated method. Developed customized scripts for Windows Server 2008 R2 & Red Hat Enterprise 6 to extract system configuration for security baseline assessment. Performed vulnerability assessments on multiple IT & OT (SCADA) enclaves. Performed security assessment utilizing the NISTIR 7628 (Guidelines for Smart Grid Cyber Security.) controls against the system. Developed technical reports to address discovered & confirmed system vulnerabilities. Vulnerability Analyst CGI Federal May 2012 to Present Currently supporting the PENCERT (PENTAGON CERT) as an active member of their CNDSP (computer network defense service provider) team. Core focus is providing vulnerability assessment on DOD wide systems using various tools and methodology. Conducting operating system, application, and database vulnerability assessments on various DOD Information Systems. Utilizing eEye's Retina vulnerability scanning tool for vulnerability assessment efforts against multiple platforms including OS (Windows XP & 7), Windows Server (2003 & 2008), Network Devices (Cisco switches/routers & Juniper switches/routers), Linux (Red Hat), and databases (Oracle & MSSQL). Verifying results and eliminating false positives to ensure accuracy for a clear understanding of the threat landscape affecting the CNO of DOD assets. Generating vulnerability assessment reports based on findings from scan results, and developing mitigation strategy for discovered vulnerabilities. Operating, maintaining and configuring Retina scanner. Configuring Retina scanners for specific scan profiles. Applying regular updates from the vendor. Training new team members of the PENTCERT on the vulnerability management program. Training junior staff on vulnerability scanning. Creating and updating SOPs and on frequent basis. In-depth knowledge and experience of DOD policies and procedures to include DOD CIO polices, interacting with US CYBERCOM and DISA for IA & Cyber

related issues. Scanned tens of thousands of systems and verified thousands of vulnerabilities for the DOD including DOD IG, DTSA, DTMP, PVDCAPS, PDAPS, DHHQ, and more Security Analyst BTC February 2012 to Present Supported IATO & ATO C&A efforts for DoD DHHQ BRAC project. Certifying classified (SIPRNet) environment consisting of hundreds of devices. Ensuring devices were in compliance with STIG. Audited devices that included servers (Windows Server 2008 R2, ESX), network devices (Cisco routers/switches layer 2 & 3, Juniper routers/switches layer 2 & 3) security devices (Juniper SIEM, SourceFire IDS/IPS, Palo Alto Firewalls), workstation (Windows 7), applications (Active Directory, Office 2010), and other devices (Cisco VTC, Cisco UCS, InfoBLOX, OpenGear). Performed vulnerability scan using Retina, HP WebInspect, and AppDetective. Performed IV&V of 8500.02 Checklist. Review and edit documentation (DIP, SIP, PSS, POA&M, system policies) Conducted surveys to determine and improve the use of documentation. IT Security Consultant HKPS July 2010 to February 2012 Developed and updated the System Security Plans, documentation review, observation and reviewing the results of technical tests. * Conducted audit interviews, control testing for (NIST, ISO 27001, and SOX) to create and produce Security Assessment and Risk Assessment. * Performed testing using a streamlined methodology and customized tools in addition to Nessus vulnerability scanning. * Coordinated Network Scanning Assessment efforts. * Performed network discovery and mapping, vulnerability scanning using tools such as Retina, Nessus, Nipper, and Acunetix Web Vulnerability Scanner. * Participated in weekly stakeholder meetings. IT Risk Auditor RGP June 2006 to November 2010 Audited system using a wide variety of security practices such as ISO 27000, SOX, HIPAA, and FISMA (NIST). * Tested compliancy of system using automated and manual methods. Utilized several security tools such as Nessus, Retina, ISS, CIS benchmark, and more. Manually checked configuration of servers (Windows 2003/2008 & Linux) and databases (MySQL, Oracle, and MSSQL) to ensure the servers were in compliance with hardening guides. * Performed application security reviews. Assessed controls to ensure adherence to corporate policies and industry best practices. * Coordinated of Application Security Assessment (ASA) activities, interfacing with the application development, business and central technology groups to ensure application compliance. * Performed and assist

in application risk activities including risk assessments, audit remediation and security testing. * Provided IT Risk guidance based on banks Standards and Policies to Application Development and project teams. * Created all boundary System Security Plans, including the tracking and close out of POA&M's. * Provided Corrective Action Plans to the Government Management Team. * Developed IT security policies, guidelines, baselines, and procedure for the Redskins organizations to reflect IT governance adherence (SOX). Education AS in General Education Henry Ford Community College - Dearborn, MI June 2011 Film New York Film Academy - New York, NY March 2002 Additional Information Skills Security Scanners: Nessus, Retina, Acunetix, AppDetective, HP WebInspect Security Standards: DIACAP 8500.1, 8500.2, NIST 800-37, NIST 800-53, SOX, FISMA, ISO 27001

Name: Mrs. Tasha Luna DVM

Email: stewartjason@example.net

Phone: 481-758-4158x80271