IT Security Consultant for Nippon Telegraph Telephone America (NTT America) IT Security Consultant for Nippon Telegraph Telephone America (NTT America) IT Security Consultant Ashburn, VA I have 12 years of FISMA Assessments experience, Security Assessment & Authorization (SA&A) and Security Test and Evaluation (ST&E), as a contractor to the US Government and 24 years of experience working for international private banks and insurance companies, in the security environment. My background has trained me to make strong and sound business decisions where the securing of customer information is paramount. I have led several Contingency and Disaster Recovery exercises. I established continuous monitoring procedures based upon the best practices of ST&E. I have successfully completed FIPS-199, NIST SP800-53, Sarbanes-Oxley, HITRUST, and Payment Card Industry (PCI) compliance projects. I especially like to write Procedures, Policies, and Opinions. Authorized to work in the US for any employer Work Experience IT Security Consultant for Nippon Telegraph Telephone America (NTT America) NextGen Information Services, Inc - Herndon, VA January 2019 to May 2019 NTT America brought me in to prepare them to pass the PCI Compliance Audit. Starting in early January, I was given six (6) weeks to prepare for the arrival of the Auditors. The Auditors have come and gone, I was very busy remediating the issues that were found. My contract ended on May 31, 2019. Familiarize myself with the hosting environment and NTTA s business model. Reviewed the security policies and procedures. Updated existing documents where possible. Wrote new policies and procedures, detailing is governed by the severe timetable given to me. Preparing the stakeholders for their interviews by the auditors. Contacted the auditor, to agree upon the ground rules to be followed by all during the audit. Worked with the auditor s as they interviewed the stakeholders. Started remediation work. Started HITRUST Compliance Project. Prepared final PCI evidence for submission to the auditor. IT Security Engineer Computer World Services Corp - Fairview Heights, IL December 2017 to January 2019 for the Office for the Department of the Treasury CWS won the contract with the Office of Financial Research (OFR) at the US Treasury. I work with one other IT Security Engineer, our tasks are to certify newly built server before they are allowed into the production environment. Conducting Linux and Windows server security assessments.

Conducting continuous monitoring of the servers in the enterprise environment. Creating and tracking POA&Ms from the server security assessments. Maintaining new server security assessment process. ? Document version control ? Assessment Form template (using strict version control) ? Instructions on how to complete the Assessment Form ? Periodically updating the templates and instructions, using the engineer's feedback and my own observations. Using Nexpose and Splunk for server security assessments Contributing as a team member in the Continuous Monitoring of the OFR major IT systems. Updated the User Software Request procedures Tasked with doing the Security Review of the User Software Requests, average five (5) per day Updated the procedures for the Security Review for the Importation of External Data. Tasked with the Security Review of the Importation of External Data. Support OFR's Contingency Planning Table Top exercise. Writing Python analytical programs to reduce server assessment workload. Creating Dashboards in Splunk IT Security Consultant VMD System Integrators, Inc - Reston, VA April 2014 to December 2017 for the Office for the Department of the Treasury Worked on VMD's contract with the Office of Financial Research (OFR) at the US Treasury. I worked with a team of six (6) people, our tasks were to re-certify their IT systems and to provide support in general practices. We were awarded a three (3) year contractual extension in September 2016. However, due to budgetary changes, OFR decided to re-compete the contract in May 2017. VMD decided not to participate in the rebidding. Performed Security Assessment & Authorization (SA&A) and Security Test and Evaluation (ST&E) of OFR's environment Conducted Linux and Windows server security assessments. Conducting continuous monitoring of the servers in the enterprise environment. Creating and tracking POA&Ms from the server security assessments. Created a new server security assessment process. ? Established document version control ? Updated the Assessment Form template (using strict version control) ? Wrote the procedures on how to complete the Assessment Form ? Trained four (4) security engineers in the assessment process ? Periodically updated the templates and instructions, using the engineer's feedback and my own observations. Used Nexpose for and Splunk for server security assessments Proposed improvements to the Change Control process. Contributed as a team member in the Continuous

Monitoring of the OFR major IT systems. Updated the User Software Request procedures Tasked with doing the Security Review of the User Software Requests, average five (5) per day Updated the procedures for the Security Review for the Importation of External Data. Tasked with the Security Review of the Importation of External Data. Prepared OFR's Contingency Planning Table Top exercise. Wrote JIRA, firewall logs and server logs analytical programs using Python Wrote a procedure and flow-chart for the handling of JIRA issues tickets. Creating Dashboards in Splunk IT Security Consultant Agensys Corporation - Ashburn, VA October 2013 to April 2014 for the Office for the Department of the Treasury $60 per hour This was a "6 month to hire" position for VMD System Integrators, Inc. contract at the US Treasury. I worked with a team of six (6) people, our tasks were to re-certify their IT systems and to provide support in general practices. In April 2017, VMD invited me to join as a permanent employee. Contributed as a team member in the Security Assessment & Authorization (SA&A) of the support systems. Wrote the User Software Request procedures Tasked with doing the Security Review of the User Software Requests, average three (3) per day Rewrote the procedures for the Security Review for the Importation of External Data. Tasked with the Security Review of the Importation of External Data. Senior Information Analyst TWM Associates Inc - Falls Church, VA May 2013 to August 2013 for Fannie Mae I performed as a Consultant to the Director of Corporate Security & Resiliency, performing architecture planning in support of key Physical Security and IT initiatives. I focused on requirements and design phases, supported development, testing, and issue escalation. I managed and promoted use of Sarbanes-Oxley (SOX) IT standards, served as subject matter expert to Fannie Mae projects and provided support for project team members. The initial contract was for three (3) months, however I was asked to stay an additional month *. Created a risk assessment and security categorization process for office building entrance/exit doors. * Provided the defense against Distributed Denial of Services (DDOS) requirements for the preparation for the annual Building Security Resiliency Exercise. Security Analyst Metters Inc - McLean, VA March 2012 to March 2013 for the Federal Insurance Depository Commission (FDIC) I supported the Federal Depository Insurance Corporation (FDIC). I created an end-to-end process for evaluation of third-party system

security, including System Security Plans (SSPs) and mechanisms for handing of Privacy Act data (PII). I have also performed technical and process-driven security assessments of contracted vendors and built matrices for private sector versus US government requirements trace ability. I served as a liaison/translator for the compliance requirements of SOX and FISMA. Processing contractor security (PII & SSP) packages for the Federal Depository Insurance Corporation (FDIC) based upon ST&E methodology. Creating checklists, report templates. Recommending improvements in the Assessment Process. Conducted assessments of FDIC vendor Security policy and practices Conducted security assessments of contracted vendors. Created a process for compiling and remediation of POA&M items. Project discontinued by FDIC, the contract ended. Security Analyst for the United Sates Marshal Services Centech Group - Falls Church, VA October 2011 to March 2012 USMS) I supported the United States Marshal Services (USMS). I served as a liaison between the application and the security departments; promoted the integration of security considerations within the system development life cycle (SDLC). I maintained the system security posture during the contractor transition period. I coordinated two major application releases, including the design and testing of contingency plans for operational continuity. Maintained the system security posture during the transition Continued to Liaison between the application group and the Security Department. Coordinated two major application releases by ensuring all preparations were ready. Coordinated a contingency test of the primary application. Security Consultant for the United Sates Marshal Services Altron Inc - Arlington, VA February 2010 to October 2011 USMS) I supported the United States Marshal Services (USMS). I led an initiative that raised the USMS Foundstone score from 30 to 95 in three months, and I am proficient in the development of security risk metrics. I wrote the system security baseline for Red Hat 5 Linux CIS compliance scans and authored and administered a FISMA-compliant Annual Security Awareness Program. I served as principle liaison between the JDIS (operations) and audit teams. I planned the continuity of operations and contingency activities. I drafted Service Level Agreements (SLAs) and Memorandum of Understanding (MOUs). Led the campaign to raise the Foundstone score from 30 to 95 during a three month period. Wrote the RedHat 5 System Security Baseline, for the CIS

compliance scans. Authored and administered the Annual Security Awareness Program so that the USMS could satisfy the Federal Information Security Act (FISMA). Liaised between the JDIS team and the Auditors for the ST&E process Resolved outstanding POA&M items. Wrote the system contingency plan. Wrote and updated, Service Level Agreements and Memorandum of Understanding Altron lost the USMS contract to Centech Group. Security Analyst to the Federal Communications Commission Open Systems Sciences Inc - Newington, VA October 2007 to February 2010 FCC) I supported the Federal Communications Commission (FCC) conducting Certification and Accreditation (C&A) of systems and applications to include Microsoft Windows, Solaris UNIX, and various "flavors" of Linux, TCP/IP-based network hardware such as Firewalls, Routers, and Switches. I developed technical risk assessment methodologies leveraging guidance from the Center for Internet Security (CIS) and National Security Agency (NSA). I conducted the Certification and Accreditation of the systems and applications, used by the FCC (Windows, Solaris, Linux, Sybase, TCP/IC, Firewalls, Routers, Switches, etc.). I wrote the procedures for the C&A team's ST&E process (800-60, 800-53, 800-37, 800-53a, and POA&M remediation). Senior Analyst to the Federal Communications Commission TWM Associates Inc - Falls Church, VA April 2006 to October 2007 FCC) and Freddie Mac I conducted the Certification and Accreditation (C&A) of the Integrated Spectrum Auction System (ISAS) for Federal Communications Commission (FCC) Spectrum Management and Resource Technology (SMaRT) Division of the Wireless Telecommunications Bureau (WTB). I updated the existing Security Policies and authored several new policies as requested by the customer. While at Auctions, I prepared the security policy for three (3) audits, "Integrated Spectrum Auction System (ISAS)", "Universal Licensing System (ULS)", and "Auctions Network". I monitored the network vulnerability scans and ensured that patches and updates were done. I monitored the security portion of the auctioning of several wireless frequencies. I was an active contributor to discussions, planning, and implementing of new security systems and tools. For Freddie Mac, I wrote the SOX Compliance Review policy covering TWM's activities at Freddie Mac, along with overseeing the creation of the Freddie Mac SOX Compliance Review Procedural Instructions. I supported the Team Lead's presentation on SOX to Freddie Mac

Management. Freddie Mac: Wrote the SOX Compliance Review policy and instruction. Federal Communications Commission (FCC): Updated the existing Security Policies and authored several new policies. From August 2006 to August 2007, prepared the security policy for three (3) audits. TWM lost the FCC contract to Open System Sciences Chief IS Security Officer Monro Muffler Brake - Rochester, NY December 2004 to September 2005 I wrote and compiled their new Information Technology Security Policies, covering their AS400, MS Servers, Desktops and Network for IT Security SOX compliance objectives. This task required me to be responsible for the evaluation of Monro's IT security policies (pre-auditing) and creating a test plan to ensure compliance, the effort to audit and test all IT Security SOX compliance objectives. I determined the Test Scenarios for the controls by which would insure that compliance objectives could be verified; then I tested over 50 test cases and provided analysis for appropriate remediation. I reviewed suggested remediation for all Security concerns found weak. These resolutions were based on recognizable "Best Practice", as recommended by SANS.org, US-Cert, InfoSysSec, COBIT, and other valid security resources organizations. Based upon the solutions and the test results, I wrote the IT Security policies and Standards based on test results. I was responsible for presenting the IT Security summation of disposition of overall status to the external auditor. I started a global Internet awareness campaigned by asking, "Where is Paris?" and answering, "It's on the other side of your Enter key". I mapped out the remediation effort to meet the Visa PCI compliance requirements. This required me to evaluate the security standards for the "Safe Keeping" and transmission of the customer credit card information. I mapped out the flow of data, identified the vulnerable points, and suggested appropriate remediation, such as employing an encryption method. Wrote and compiled new Information Security Policies, covering the AS400, MS Servers, Desktops and Network for IS Security SOX compliance objectives. Mapped out the remediation effort to meet the Visa PCI compliance requirements. Hosting Manager / Security Consultant S1 Corporation - Singapore January 2001 to August 2004 I extensively revised the "S1 Singapore Internet Banking Security Policy" to meet the security standards of the Monetary Authority of Singapore (MAS). The policies were passed by 3 independent auditors and by the MAS. Deputy Security Manager United

Overseas Bank Group - Singapore October 1996 to January 2001 I secured the bank's first Internet Banking WEB site. I then planned and implemented a bank-wide Internet/Intranet security policy encompassing 14 local and global sites requiring the deployment 21 Firewalls. I was a participant in formulating the Monetary Authority of Singapore's (MAS) "Internet Banking Security Guidelines". I wrote several security white papers, instrumental in convincing the bank's board of the need to establish a strong eCommerce security policy. I wrote and revised the corporate LAN, AS400, and Mainframe security standards. I set up a VPN environment, and conducted audits of the firewalls and eCommerce servers. I was also responsible for preparing and conducting courses on the security of products used by the bank. Established the Internet security policies and secured the bank's first Internet banking site. Planned and implemented a bank-wide Internet/Intranet security policy encompassing 14 local and global sites requiring the deployment of 21 Firewalls. Installed and administered a PGP certificate server. Conducted annual audits of the firewalls and eCommerce servers. Regional Operations Support Analyst American International Assurance - Singapore March 1995 to October 1996 I oversaw an AS400 locally in Singapore with a link to an IBM Mainframe in Hong Kong. I wrote and maintained the Guidelines and Policies covering System Security and Help Desk procedures. I was responsible for managing the annual AS400 Disaster Recovery Exercise. Responsible for managing the annual AS400 Disaster Recovery Exercise. Senior Operations Specialist Transamerica Life Companies - Los Angeles, CA August 1980 to February 1995 My duties included data communications, IMS online administration, and Mainframe System Programming. I wrote SAS programs to review and report all the areas in production control, lead the operations staff in exercises to testing the Mainframe Disaster Recovery Plan. I installed Token Ring LANs in the Transamerica center, along with configured the systems for controlling modems in a System Network Architecture (SNA) environment. 15 years of tremendous growth in the Information Technology Division IBM 390 Mainframe. Education University of Fairfax 2008 University of California at Los Angeles (UCLA) - Los Angeles, CA 1986 to 1995 High School Diploma Brick Township High School 1971 Ocean County College 1971 Skills IMS (10+ years), LINUX (8 years), MAINFRAME (10+ years), AS400 (7 years), SAS (10+ years), Information

Security, It Security, Cissp, Siem, PCI Links http://www.linkedin.com/in/stephenharashack Certifications/Licenses Certified Information Systems Security Professional (CISSP) August 2009 to Present Certified Information Systems Security Professional (CISSP) Certificate/ID number: 111072 August 10, 2009 Additional Information TECHNICAL SKILLS Operating Systems: Red Hat 6 Linux; HP Unix 11; Windows 2000, NT4, XP, 98 & 95; Sun Solaris 7, 8; AS400; IBM MVS; JCL; COBOL; Top-Secret Assessment Tools: Nexpose; Splunk; Foundstone; WebInspect; Nessus Hardware: DELL servers & desktop; SUN Servers (10 & 240); HP 9000 Servers (A, K, L, N & R Class); IBM (AS400 & Mainframe); Cisco (Routers, Switches and PIX) Applications: Norton Corporate Anti-Virus; Dream Weaver; IBM WebSphere; HP OpenView, ClearQuest, Splunk Databases: Dbase; MS SQL (6.5 & 7); Informix (7.3 & 9.2); Oracle 11g; IBM (IMS & CICS) Backup Tools: Veritas Netbackup4.5; Legato Networker; HP Omniback Programming: Python 3.4, SAS Technical

Name: Elizabeth Fleming

Email: ochoi@example.net

Phone: 572-946-5201x6687