Cybersecurity Policy Analyst/Independent Consultant Cybersecurity Policy Analyst/Independent Consultant Cybersecurity Policy Analyst/Independent Consultant - MindPoint Group, LLC Work Experience Cybersecurity Policy Analyst/Independent Consultant MindPoint Group, LLC October 2015 to Present Agency: Department of Justice Location: DOJ Facilities in the Washington, DC metropolitan area Summary: Review and analysis of audit findings and develop appropriate documentation to reflect schedules and milestones of corrective activities. Provide resources to perform information assurance activities to support the advancement of DOJ's IT Security Program and related IT Program areas. Possess working mastery of the DOJ Cyber Security Assessment and Management (CSAM) security program management application and responsible for ensuring that Components understand and comply with the Department's IT security requirements. Responsible for knowing all applicable Federal IT Security mandates, how and where these mandates tie into DOJ orders, policies, instructions, handbooks and guides, and the impact of the security requirements on Component systems and mission. Responsible for Component IT security activities and compliance, and provide hands-on assistance as appropriate to ensure Component success. ? Conduct formal Office of the Chief Information Officer system oversight review, provide feedback and document findings in CSAM. Provide hands-on assistance to Components to correct weaknesses as necessary. ? Ensure Component hardware and software inventory and documentation is accurate and current for FISMA reporting. Ensure Component security authorization boundaries are properly defined and captured in the system security plans, and that all interconnection agreements are in place and current. ? Ensure Component system security authorization controls contain accurate implementation statements (formerly compliance descriptions) ? Ensure Component systems offer appropriate controls for inheritance and the inheriting systems inherit only what's appropriate ? Support Components with annual recertification of accounts - ensure new accounts have appropriate forms (and signed by appropriate approving authority) and any inactive accounts are deactivated in accordance with DOJ policies. ? Ensure Component system scanning takes place in accordance with the Department's plans and schedule. ? Ensure Component systems have secure configuration baselines set and documented, and any

deviations approved by the authorizing official.  ? Ensure all audit Notification of Finding and Recommendation are entered into CSAM as a POAM. Ensure Component system POAMs have appropriate milestones, accurate description of the weaknesses and remediation, task owners, estimated cost to completion and realistic due dates.  ? Ensure all systems update their annual incident response and contingency plans, conduct the appropriate training, document the appropriate POCs, and document the after action plans.  ? Ensure Components reach their CSAT and IT Professional training completion targets on time.  ? Support Federal data calls relating to classified and unclassified systems. Security Engineer/Independent Security Assessor Securicon - Alexandria, VA September 2013 to October 2015 Summary: Served Securicon's Risk Management Services customers, primarily supporting Federal FISMA programs. Conducted assessment and authorization tasks, including independent security assessments, risk analyses, security test plans and assessment reports in support of Securicon's customers' Risk Management Framework programs under NIST, OMB and other related guidelines. Served as Project Lead and provides training, guidance, and quality assurance for intermediate and junior information security analysts.
? Measured information assurance by conducting annual risk assessments of the management, technical and operational controls of various general support systems and major applications to determine if the security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements of the organization.  ? Prepared security assessment kick-off activities by creating corresponding security documentation such as the security test and assessment (ST&A) and security requirements traceability matrix (SRTM)  ? Assessed applicable system security controls including identified DOC volatile controls on an annual basis to support the re-authorization decision and comply with FISMA Assessments & Authorization (A&A) requirements  ? Utilize various NIST and FIPS publications such as 800-53a rev.4 , 800-37 Rev.1, 800-53 rev. 4, 800-115, 800-39, FIPS 140-2 and FIPS 200  ? Schedule, lead, and coordinate security assessment activities such as security assessment interviews, package handoffs to ISSOs and artifact/evidence deadlines  ? Coordinate with System Owners and ISSOs to gather applicable artifacts (screenshots, system documentation, live observation, etc)  ? Create

security assessment reports upon completion of security assessments ? Verify completion of a Security Impact Analysis (SIA) for all major system changes and ensure no deviations within the security authorization boundary and system documentation ? Ensure system authorization boundaries are updated to reflect the most recent system architectures requirements for Federal Information and Information Systems ? Responsible for QA of assessment team deliverables, provide feedback and support on security assessments for team members and oversee team members as the designated Project Lead for various assessment packages ? Provide training, guidance and quality assurance for mid-level and junior information security analysts. Advise ISSOs of system scoping, countermeasures and mitigation recommendations based on architectural/technology considerations and assessment ? Provided ad-hoc support to the Program Manager by assisting in annual assessment schedules and weekly reports IT Security Analyst/Independent Security Assessor Missing Link Security - Alexandria, VA May 2011 to August 2013 Summary: Performed Security Assessment & Authorization (SA&A) activities with minimal supervision. Configured and launched compliance and vulnerability scans during quiet time on workstations, databases, URLs, servers and applications and compiled reports for analyzing/mapping. Responsible for quality assurance (QA) of assessment team deliverables, provided feedback and support on security assessments for team members and oversee team members as the designated Project Lead for various assessment packages. ? Created security test and assessment (ST&A), security assessment reports (SAR) and security requirements traceability matrix (SRTM) for various USPTO information/financial systems by analyzing information system/vendor documentation such as System Security Plans (SSP), High-Level Architecture (HLA), Detailed Design Document (DDD), Operational Support Plans (OSP) and commercial off the shelf products (COTS) manuals such as installation guides ? Interviewed information system point of contacts to include Technical Leads (TL), System Owners (SOs), and ISSOs ? Tested the implementation of security controls and reviewing, validating and applying quarterly vulnerability and compliance scan results to assessments ? Ensured the consistency, accuracy and continuity of all information as it pertains to the ST&A plan, SRTM, SAR and all evidence utilized during the

assessment is complete, consistent, and compliant with all applicable and mandatory requirements. These applicable and mandatory requirements include but are not limited to: FISMA, OMB, IT Security and Privacy policies and implementation guidance for the Executive Branch, SDLC, NIST, FIPS Publications and agency policies ? Obtained relevant information system security documentation/information/screenshots relevant USPTO information systems and utilized Cyber Security Assessment and Management (CSAM) ? Configured and launched compliance and vulnerability scans during on workstations, databases, URLs, servers and applications and compiled reports for analyzing/mapping using Tenable Nessus, Appdetective DB Protect and AppScan, which aids in assessing the security posture of the system Junior IT Security Analyst/Independent Security Assessor Syneren Technologies - Alexandria, VA January 2011 to April 2011 Summary: Worked on a team responsible for performing/managing security related tasks for the USPTO network security infrastructure. ? Became familiar with NIST Special Publications 800 Series: 37 Rev.1,53 Rev.3, 115, 39, 53a. Also, became familiar with FIPS 140-2 compliance and FIPS 199. ? Conducted extensive review/research of Detailed Design Documents (DDD), Configuration Management Plans (CMP), Operational Support Plans (OSP), Contingency Plans (CP) and vendor documentation. ? Conducted assessment interviews with Technical Leads and System Owners using NIST guidelines and Senior leadership ? Staged discussions with individuals to facilitate understanding, achieve clarification, or lead to the location of evidence/artifacts. Established appropriate communication channels among organizational officials/senior leadership having an interest in the assessment. IT Security Intern George Mason University - Fairfax, VA November 2008 to December 2010 Worked with the IT Security Unit and monitored status of all computers connected to the George Mason University network (Arlington, Fairfax and Prince William Campus) using NitroSecurity's NitroView Intrusion Prevention System (IPS), Symantec Endpoint and FireEye Malware Protection ? Compiled relevant information about flagged systems and filed incident tickets using software such as BMC Service Desk Express ? Resolved compromised email accounts due to phishing attacks by contacting and discussing sensitive information with faculty/waged students. ? Communicated proper security practices and awareness to victims such as utilizing stronger passwords and noticing

suspicious emails/attachments ? Wiped, installed, troubleshoot, secured, updated and encrypted hard drives/operation systems/anti-virus using software such as Sophos Encryption and Darik's Boot and Nuke (DBAN) ? Reviewed on a daily basis alerts and vulnerabilities from the US-CERT and Common Vulnerabilities and Exposures (CVE) Education Bachelor of Science in Information Security George Mason University - Fairfax, VA Skills Security, Fisma, Nist, Sop, Audit, Remediation, Test coordination, Pbc Additional Information PROFESSIONAL EXPERTISE ? FISMA/FISCAM Compliance/Reporting ? Authorization to Operate/Test Coordination ? POAM/NFR Management/Remediation ? CSAM Administration/Oversight ? Security Control Assessments/Scoping ? Stakeholder Engagement/PBC Organization ? Policy/Memo/Waiver/SOP Development ? Audit Preparation (IG/Independent 3rd Party) ? Artifact/Implementation Statement Review ? NIST (37, 53a and Rev4) FIPS (199. 200)

Name: Terri Lee

Email: hamiltonrichard@example.net

Phone: (930)216-9001x3749