Sr. IT Security Specialist Sr. IT Security Specialist Sr. IT Security Specialist - United State Dept. of Agriculture (FSA) Greenbelt, MD Skilled Information Security Specialist with expertise in risk management framework (RMF), systems development life cycle (SDLC), risk management, and vulnerabilities management of a wide range of vulnerabilities and threats. Well-versed in direct and remote analysis with strong critical thinking communication and people skills. A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Able to thrive in fast-paced and challenging environments where accuracy and efficiency matter. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring for government (FISMA & NIST) and commercial clients. Authorized to work in the US for any employer Work Experience Sr. IT Security Specialist United State Dept. of Agriculture (FSA) - Kansas City, MO November 2018 to Present Selected Responsibilities - Developed, reviewed, and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200 and OMB A-130 Appendix III - Provided security expertise and guidance in support of security assessments - Supported A&A (C&A) activities according to the A&A project plan - Reviewed authorization documentation for completeness and accuracy for compliance - Facilitated Security Control Assessment (SCA) and Continuous Monitoring Activities - Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4 - Ensured cyber security policies are adhered to and that required controls are implemented - Validated information system security plans to ensure NIST control requirements are met - Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR) - Authored recommendations associated with findings on how to improve the customer's security posture in accordance with NIST controls - Assisted team members with proper artifact collection and detail to clients examples of artifacts that will satisfy assessment requirements - Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies - Updated and reviewed A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, POA&M, BIA, PTA, PIA, and more Sr. Information Security Analyst Dept. Of Labor - Washington, DC November 2016 to November 2018 Selected Responsibilities - Facilitated Security Control Assessment (SCA) - Assessed security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements - Produced security assessment report that documents the results of assessments - Provided Security Engineering, on an as needed basis, to support to the Security Controls Assessors (SCAs) and Validators for A&A and C&A efforts, respectively - Performed security assessments; design reviews; and provide guidance on new technologies for Fleet customers. New technologies may include, but are not limited to, Cloud technologies, Hardware, Operating System, Web technologies, and Databases - Designed, developed, integrated, tested, implemented, deployed and performed operations & maintenance (O&M) of tools for automation of security testing in support of C&A/A&A - Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR) - Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network Sr. IT Security Analyst Department of Interior - Washington, DC June 2016 to September 2016 Selected Responsibilities - Developed, reviewed, and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200 and OMB A-130 Appendix III - Provided security expertise and guidance in support of security assessments - Supported A&A (C&A) activities according to the A&A project plan - Reviewed authorization documentation for completeness and accuracy for compliance - Facilitated Security Control Assessment (SCA) and Continuous Monitoring Activities - Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4 - Ensured cyber security policies are adhered to and that required controls are implemented -

Validated information system security plans to ensure NIST control requirements are met - Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR) - Authored recommendations associated with findings on how to improve the customer's security posture in accordance with NIST controls - Assisted team members with proper artifact collection and detail to clients examples of artifacts that will satisfy assessment requirements - Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies - Updated and reviewed A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, POA&M, CPTPR, BIA, PTA, PIA, and more - Collected Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless - Uploaded supporting docs in the System's Artifact Libraries, Google Docs, and CSAM - Updated, reviewed, and aligned SSP to the requirements in NIST 800-53, rev4; so that assessments can be done against the actual requirements and not ambiguous statements IT Security Analyst Dept. of Veterans Affairs - Washington, DC May 2013 to June 2016 Selected Responsibilities - Developed, reviewed and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Apply appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200 and OMB A-130 Appendix III - Coordinated and managed team activities during assessment engagements - Established schedules and deadlines for assessment activities - Held kick-off meetings with CISO and systems stakeholders prior to assessment engagements. - Prepared and submitted Security Assessment Plan (SAP) for approval - Developed and update security plan, plan of action and milestone (POA&M) - Monitored controls post authorization to ensure continuous compliance with the security requirements - Managed vulnerabilities with the aid of Retina, and Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network - Prepared and reviewed documentation to include SSP, SAP, SAR, POAM Packages - Created reports detailing the identified vulnerabilities and the steps taken to remediate them - Reviewed and Updated some of the Artifacts especially

FIPS 199, Initial Risk Assessment, e-Authentication, PTA, PIA, SAR, POAM - Developed, evaluate and implemented information security governance processes, including policies, standards, procedures and risk management practices - Implemented governance frameworks and security risk management processes, such as NIST, ISO, OMB guidelines and standards Education Bachelor of Science in Computer Science Lagos State University - Lagos, NG 2004 Information systems and developed Security NIST Skills Information Assurance (Less than 1 year), Risk Assessment (3 years), Security (6 years), security policies (Less than 1 year), System Security (4 years), access, testing, HTML, Active Directory Additional Information CORE COMPETENCIES ? Assessment and Authorization (A&A) ? Certification and Accreditation (C&A) ? IT Security Compliance ? Vulnerability Assessment ? Vulnerability Scanning ? Information Assurance ? Security Control Assessment (SCA) ? Patch Management ? Risk Assessment ? Systems Development Life Cycle ? Technical Writing ? Project Management and Support ? Project evaluations ? Analysis and reporting ADDITIONAL SKILLS Ability to establish and maintain effective working relationships with clients and co-workers Skills in interviewing users to help analyze and resolve issues Strong organizational, analytical and planning skills Ability to read and interpret system security policies, rules and regulations Strong communication (verbal & written) and presentation skills Ability to communicate security and risk-related concepts to both non-technical and technical audiences

Name: Michael Holland

Email: pkaufman@example.net

Phone: 001-266-810-7671x401