IT Security Analyst IT Security Analyst IT Security Analyst - NOAA Lanham, MD Skilled Information Security Analyst, knowledgeable in risk management framework (RMF), systems development life cycle (SDLC), security life cycle, and vulnerabilities management using FISMA, and applicable NIST standards. Organized, Solutions-focused, deadline-focused, team oriented, work well independently, or in team providing all facets of computer supports with in-depth knowledge and understanding of numerous software packages and operating systems. A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring for government and commercial clients. Functional areas of expertise include: Assessment and Authorization (A&A) IT Security Compliance Vulnerability Assessment Vulnerability Scanning Security Test and Evaluation (ST&E) Certification and Accreditation (C&A) Risk Assessment Systems Development Life Cycle Technical Writing Project Management and Support TECHNICAL AND SPECIALIZED SKILLS Nessus Vulnerability Scanner, Microsoft Office, Excel, Word, PowerPoint, MS Project, Access, Mac, Microsoft Windows, Linux, VMware, Oracle virtual box, Parallel Virtual Machine, CSAM, RSAM, Tripwire, Accellion/WatchDox secured file solution, RMPS, Remedy, Splunk, Active Directory, ServiceNow, Trend Micro, and more. Authorized to work in the US for any employer Work Experience IT Security Analyst NOAA - Suitland, MD September 2015 to Present - Supported client Security policies and activities for networks, systems and applications including Vulnerability Management, Incident Reporting, Mitigation, and Continuous Monitoring - Supported all Assessment and Authorization (A&A) phases and processes - Proven ability to support the full life-cycle of the Assessment and Authorization (A&A) process - 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 - Direct experience with formatting, customizing, and providing feedback for documentation relating to Information Assurance & IT Security Vulnerability - Provided security

expertise and guidance in support of security assessments. - Supported A&A (C&A) activities according to the A&A project plan - Review, analyze and evaluate business system and user needs, specifically in Authorization and Accreditation (A&A) - Perform internal audits of the systems prior to third party audits - 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 - 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 - 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 - Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single, and multiple assets across the enterprise network - Reviewed SAR post assessment; created and completed POAM's milestones to remediate findings and vulnerabilities - Monitored security controls post authorization to ensure continuous compliance with the security requirements IT Security Specialist Vinds Inc - Laurel, MD March 2014 to September 2015 - 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 Education Bachelor's in Computer Science Ladoke Akintola University of Technology - Nigeria September 2006 to September 2011 Skills SECURITY POLICIES, SYSTEM SECURITY, INTERVIEWING, PRESENTATION SKILLS, testing, Active Directory, access, security, Microsoft Office, training, SQL, HTML, Sharepoint, Cisco Certifications/Licenses CISSP in progress

Name: Devin Tate

Email: tfernandez@example.net

Phone: +1-327-242-3660x4389