Senior Information Security Analyst Senior Information Security Analyst Senior Information Security Analyst - Dallas Children's Medical Center Dallas, TX Work Experience Senior Information Security Analyst Dallas Children's Medical Center - Dallas, TX January 2016 to Present Risk Management Framework (RMF) assessments and Continuous Monitoring: Performed RMF assessment on several different environments at the AITC using both scanning tools and manual assessment. Assessment included initiating meetings with various System Owners and Information System Security Officers (ISSO), providing guidance of evidence needed for security controls, and documenting findings of assessment Current Governance, Risk and Compliance tool been used is RiskVision and in transition to eMASS. NIST 800-37 risk management framework - categorize systems, privacy impact assessments, security impact assessments, interconnection security agreements, risk assessments, waivers. Develop and manage the contract/program's security documentation such as System Security Plans (SSP), Security Risk Assessment Reports (SAR), test and evaluation reports, security policies, contingency plans, Plan of Action and Milestones (POAM), and incident response plans Work on a project basis to address Community Referral Documentation Program and LAMP compliance as mandated by HIPAA Security and Federal & State Regulations as well as new regulatory and/or company-established requirements. Conduct third-party vendor risk assessments based on industry security standards and internal risk management policies. Execute LAMP HIPAA Security Compliance Program, including perform assessments of new and existing application systems, and provide monitoring of remediation efforts by the business units. Perform analysis to identify security gaps and deficiencies trends and report compliance risk/deficiencies to management Maintain the contract/program's Security Management and Reporting Tool (SMART) process and coordinate with the SMART working group to add, modify and/or remove existing applications Review authorizations to Transfer Sensitive Data (ATSD) and ensure they are process per standard operating procedure Develop and maintain standard operating procedures (SOP) for the contract/program's application suite Provide user support which includes GRC training, Tier-2 application support, user account management, and recertification of user access entitlements Principal Cybersecurity Analyst American College of

Emergency Physicians - Irving, TX June 2013 to December 2016 Conducted walk-through, formulated test plans and testing procedures, document gaps, test results, and exceptions and develop remediation plans for each area of testing NIST 800-37 risk management framework - categorize systems, privacy impact assessments, security impact assessments, interconnection security agreements, risk assessments, waivers. In depth experience in security incident response and management including analysis of events, review of suspected malicious activity, identification of Indicators of compromise and providing guidance on resolution and remediation activities Executed technical risk assessments, advise business and IT leaders on risk of initiatives Defined and executed Third Party / Vendor Information Security Risk Assessment programs Supported organization's Business Continuity Plan (BCP) and Disaster Recovery (DR) processes by evaluating resilience, recovery capabilities and risks inherent in their IT infrastructures for strategic purposes based on ISO 27001 and NIST Special Publications 800-34 series Experienced designing and implementing controls within corporate networks to include computer/network security and operating systems such as UNIX, Linux, and WINDOWS, as well as LAN/WAN internetworking protocols such as TCP/IP and network perimeter protection (firewalls) Participated in POA&M remediation by evaluating policies, procedures, security scan results, and system settings to address controls that were deemed insufficient during Certification and Accreditation (C&A), RMF, continuous monitoring, and FISCAM audits. Performed assessments, POA&M remediation and document creation using ISO 27001 and NIST SP 800-53A rev4. Conducted PCI compliance testing to verify corporate PCI security controls meet the latest PCI DSS requirements. Executed the system HIPAA Security Compliance Program, including perform assessments of new and existing application systems, and provide monitoring of remediation efforts by the business units. Involved in creating System Test & Evaluation (ST&E) documents and helped review and update existing ones for multiple information systems Assisted ISSOs in creating solutions to weaknesses based on system functionality and pre-existing architecture. Oversaw the preparation of a Comprehensive and Executive Certification & Accreditation (C&A) packages for approval of an Authorization to Operate (ATO) Ensured all weaknesses discovered during assessment of security controls are completed and tested in timely

fashion to meet client deadlines. Interfaced with IT operators and network engineers to mitigate system vulnerabilities discovered in network devices. IT Auditor Cain Watters & Associates - Plano, TX July 2010 to June 2012 Performed comprehensive Security Controls Assessments (SCA) and wrote reviews of management, operational and technical security controls for audited applications and systems. Oversaw auditors to identify IT related risk throughout development phases. Areas include networks, operating systems, databases, security and disaster recovery. Performed general controls oversight and review to verify compliance with SOX provisions and professional standards. Ensured audit tasks are completed accurately and within established timeframes. Identified and evaluated risks during review and analysis of the System Development Life Cycle (SDLC), including design, testing/QA, and implementation of systems and upgrades. Lead and facilitate meetings with system stakeholders and technical personnel to categorize systems, define system boundaries, and establish and maintain information security standards and procedures in compliance with information security and risk management policies, standards, and guidelines Prepared audit scopes, reported findings and presented recommendations for improving data integrity and operations. Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with Payment Card Industry Data security Standard. Conducted security control assessments to assess the adequacy of management, operational privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with the Plan of Action and Milestones (POA&M). Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk assessments (RAs), Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs) and evaluated existing documents for correctness and compliance with applicable policies. Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 500-53 standards. Education Master of Science in Accounting University of Dallas - Irving, TX Bachelor of Business Administration in Accounting

University of North Texas - Denton, TX Skills SECURITY, IDS, IPS, SIEM, FIREWALL, INTRUSION, VISIO, SQL, MS OFFICE, INTRUSION DETECTION, EXCEL, OUTLOOK, POWERPOINT, WORD Additional Information Technical Skills * IDS/IPS, penetration and vulnerability testing * Firewall and intrusion detection/prevention protocols * Security Information and Event Management (SIEM) * Experienced in MS Office (Word, Visio, Excel, PowerPoint, Access, and Outlook), SQL, Pro Systems, and Microsoft Azure.

Name: Krystal Nolan

Email: apatterson@example.com

Phone: (973)950-9829