IT CYBER SECURITY ANALYST IT CYBER SECURITY ANALYST IT CYBER SECURITY ANALYST - HMSHost Corp Bethesda, MD Authorized to work in the US for any employer Work Experience IT CYBER SECURITY ANALYST HMSHost Corp - Bethesda, MD January 2014 to Present Responsibilities: Validate compliance with FIPS 199-200, NIST Special Publications, Risk Assessments, E-Authentication using security tools and artifacts (e.g., IPS/IDS, PTA, PIA, SORN) Ensure client solutions comply with NIST 800-53 rev4 (and rev5 soon to be released) Review and update Information System Security documentation, to include but not limited to System Security Plans (SSPs), Plans of Action & Milestones (POA&Ms), Risk Assessments (RAs) Work with ISSOs to complete timely remediation of audit findings, security planning and reporting, plus the mitigation or retirement of security vulnerabilities Review scan reports, identified critical vulnerabilities and coordinated with system owners to remediate vulnerabilities Create and review additional security artifacts (SSP, SAP, CP, PTA, PIA, SSP, Incident Response) Continuously collaborate with C-Level Executives to discover vulnerabilities and develop mitigation and remediation plans that will secure assets such as Intellectual Property and critical data; includes development of White papers, Executive briefings and presentations to Executive level clients Support the risk management process by determining and assigning risk impact ratings for systems in accordance with Federal Information Processing Standards (FIPS) 199, which determines the level of effort required for the certification and accreditation process of a system and determines the security controls for the protection of an information system Knowledge Implementing, reviewing, maintaining and monitoring Information Security Management Systems involved in International and commercial projects in accordance to ISO/IEC 2700 series (ISO/IEC 27001-27005) Contribute to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management Perform comprehensive Security Controls Assessment (SCA) and write reviews of management, operational and technical security controls for audited applications and information systems Lead team to remediate, validate, prepare and collate security artifacts in order to pass ATO audits. Results and Benefits: Adapted to meet accelerated client deadline Mitigated risk within internal review and audit reports System Security Plans (SSPs) Cyber Security Compliance Six (6) Step

RMF Process Risk Assessments (RAs) Plan of Action & Milestones NIST Security Compliance Education Some college Skills IDS (4 years), IPS (4 years), ISO (4 years), ISO 27001 (Less than 1 year), SECURITY (4 years) Additional Information Technical Skills NESSUS Scanner ISO 27001 - 27005 MS, SharePoint & PeopleSoft IDS/IPS CSAM Tracking Tool SANS 20 Acritical Security Controls PCI Compliance

Name: Taylor Noble

Email: breyes@example.net

Phone: +1-592-231-8179x00697