IT Security Analyst IT Security Analyst IT Security Analyst - National Cancer Institute Germantown, MD Authorized to work in the US for any employer Work Experience IT Security Analyst National Cancer Institute September 2013 to Present Assist System Owners and ISSO in preparing certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53rev4 Conduct kick off meetings in order to categorize systems according to NIST requirements of Low, Moderate or High system using NIST SP 800-60 Develop a security baseline controls and test plan that was used to assess implemented security controls Conduct security control assessments to assess the adequacy of management, operational, privacy, and technical security controls implemented. A Security Assessment Reports (SAR) are developed detailing the results of the assessment along with plan of action and milestones (POA&M) Develop risk assessment reports. This report identified threats and vulnerabilities applicable to assigned systems. In addition, it also evaluates the likelihood that vulnerability can be exploited, assesses the impact associated with these threats and vulnerabilities, and identified the overall risk level Assist in the development of an Information Security Continuous Monitoring Strategy to help maintaining an ongoing awareness of information security (Ensure continued effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions Participate in the development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the Information System Security Officers (ISSOs), the System Owner, the Information Owners and the Privacy Act Officer Develop E-Authentication reports following NIST SP 800-63 requirements to provide technical guidance in the implementation of electronic authentication (e-authentication) Develop/ review system security plan in accordance with NIST SP 800-18 to provide an overview of federal information system security requirements and describe the controls in place or planned to be implemented Responsible for the development of security control test plan and in-depth security assessment of NCI information systems in order to maintain HIPAA compliance by implementing guidelines and standards identified in the National Institute of Standard and Technology (NIST)

800-66 in contracted medical review facilities throughout each US state, territory and the District of Columbia Develop HIPAA compliance reports documenting audit findings and corrective actions. These reports are submitted to NCI alternate ISSO Conduct HIPAA compliance audit on behalf of the National Cancer(NCI) Institute under NIH for medical organizations that receive grants from NCI in order to evaluate compliance of administrative, physical, technical, organizational and polices safeguards Provide NCI ISSO with composite reports detailing HIPAA audit findings and recommendations to correct identified vulnerabilities Involve in the security awareness and training of staff on HIPAA requirements as it related to information technology FISMA/C&A Analyst Enlightened March 2011 to August 2013 Analyzed and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan Of Actions and Milestones (POA&M) Assisted System Owners and ISSO in preparing certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 Categorized systems based on SP -800-60 in order to select the appropriate NIST recommended control SP 800-53 Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard SOX Compliance Analyst Conducted periodic IT risk assessment and reviewed controls for any deficiencies. Deficient controls are then reported to the CISO for appropriate mitigation actions Conducted security controls assessment to ensure controls are implemented to comply with ISO standards Initiated and led information security awareness and training program in order to inform the employees of their roles in maintaining a matured security posture Contributed in weekly change management meetings in

order to evaluate change requests (systems or application) that could lead to approval or denial of the requests, validated testing results from testing environments and promoted changes to production environment Examined information security accreditation request for approval and denial Examined events logs for irregularities. Identified irregularities are then reported as incidents. The incident response process is then initiated to mitigate these irregularities Involved in security incident management in order to mitigate or resolve events that have the potential to impact the confidentiality, availability, or integrity of information technology resources. Created and maintained security metrics in order to help senior management to make decisions Provided support to internal and external audit teams as required(Helped in the gathering/presentation of evidence to validate controls effectiveness and efficiency) Interviewed departmental heads and review existing system documentations in order to define specific, measurable, agreed, relevant and theoretically sound audit objectives Education Bachelor of Science College Park USA Additional Information Perform Security Assessment and Authorization (SA&A) documentation Develop, review and evaluate System Security Plan Perform comprehensive assessments and write reviews of management, operational and technical security controls for audited applications and information systems Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A Familiar with NIST publication; FIPS 199, SP 800-60, SP 800-53rev4, SP -800-137 Excellent with COSO, COBIT, ISO, SSAE 16 (SOC1,2&3) and PCI DSS Frameworks Develop and update POA&M Ability to multi-task, work independently and as part of a team Strong analytical and quantitative skills Effective interpersonal and verbal/written communication skills

Name: Brian White

Email: xmendez@example.com

Phone: +1-754-347-9646x7680