Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst Houston, TX Authorized to work in the US for any employer Work Experience Cyber Security Analyst Northrop Grumman - Windsor Mill, MD June 2019 to Present Cyber Security Analyst Northrop Grumman (Client SSA) June 2019- Present Windsor Mill-MD Creating, updating and reviewing System Security Plans using NIST 800-18, Contingency Plans using NIST 800-34, Incident Reports using NIST 800-61 Review technical control and provide implementation response as to if/how the system are currently meeting the requirement. Work closely with Security Control Assessors (SCA) to determine effectiveness of current security controls and a path forward to implement future security controls, where potential weaknesses might exist. Perform Risk Assessment (RA) by identifying, analyzing, and reviewing documents relevant to the security controls implemented. Schedule and attend weekly meetings for audits, POA&M findings and after-action review Ensure compliance to security standards and policies, monitoring access privileges, conducting risk assessments, investigation of suspicious activities, and remediation of identified security threats or risks. Conduct security assessment by interviewing, examining, and testing the controls to see if the controls are implemented effectively, operating as intended, and producing the desired outcome. Evaluate and support the documentation, validation, assessment, and accreditation processes necessary to ensure that information technology ( IT) systems postures are secured. Make recommendations for the creation of the Plan of Action and Milestones (POA&M) for failed controls and eventual remediation actions. Prepare the A&A package by ensuring that the required documents are included such as the System Security Plan (SSP), Security Assessment Report (SAR), POA&M, Contingency Plan (CP), for the Authorizing Official (AO), to grant the ATO. Documented and review system security plan (SSP), security assessment report (SAR), security plan of action and milestone (POA&M). Participate in the security impact analysis for new, updated or changes made to the system configuration. Documenting and reviewing security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various government agencies. Maintaining and updating system security documentation as required, in accordance with agency

policies and procedures as per NIST requirements. Supporting continuous monitoring testing, and creation and management of POA&M. Ensuring risk analyses are performed accurately to determine cost-effectiveness of the security controls. Cyber Security Analyst OBXtek - Washington, DC November 2018 to May 2019 Cyber Security Analyst OBXTEK (Client -DOL) November 2018- May 2019 Washington DC Provided security expertise and guidance in support of security assessments Work with Network and Operations team to perform tests and uncover network vulnerabilities. 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 Analysis of IBM BigFix Compliance Report and review in-depth critical patch compliance report Analysis of current vulnerability type matrix, analysis of exploitable vulnerability type matrix and analysis of mitigated vulnerability type matrix Interpret IBM BigFix Web Reports Develop Continuity of Operations (COOP) and Disaster Recovery (DR) operations and conduct evaluation of COOP and DR during annual incident response training Assist the operational network team to classify and fix security bugs and mitigate risk Create a pivotal chart of vulnerabilities severity compared on a bi-weekly basis 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 client s 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 Managed vulnerabilities with the aid of Nessus Vulnerability Scanners to detect potential risks on a single or multiple asset across the enterprise network Reviewed SAR post assessment; created and completed POAM s milestones to remediate findings and vulnerabilities Independently reviewed complex security analysis of existing systems for compliance with security requirements Monitored security controls post authorization to ensure continuous compliance with the security requirements. 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. 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. Technical Subject Matter Specialist PROSOL(DOL Client) - Washington, DC December 2017 to November 2018 - 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 - Managed vulnerabilities with the aid of Nessus Vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network - Reviewed SAR post assessment; created and completed POAM s milestones to remediate findings and vulnerabilities - Independently reviewed complex security analysis of existing systems for compliance with security requirements - Monitored security controls post authorization to ensure continuous compliance with the security requirements. - 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. - Interpret IBM BigFix Web Reports Cyber Security Analyst ACE Express Corporation - Beltsville, MD November 2015 to December 2017 - 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 - 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 - Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or 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 Analyst Network Solid LLC - Silver Spring, MD May 2013 to October 2015 - Investigate use and configuration organizationally of multiple business process tools, and create gap analysis on current solution vs. ideal solution - Communicate analysis, design, and specifications both functional and technical to all supporting organizations. - Collaborate and direct efforts within Quality Assurance to ensure desired results. - Develop innovative solutions to meet the needs of the business that can be reused across the enterprise creating the environment for consolidation of

tools to robust, customizable solutions - 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. - Solve unique and complex problems with broad impact on the business - Provide time estimates at various levels of confidence for tasks from initiation through development - Identify dependencies across programs, milestones, systems, and solutions - Coordinate effort across business, technical, and program teams Oracle DBA Cystic Fibrosis Foundation - Cockeysville, MD July 2012 to March 2013 - Manage Oracle production and test databases running on Linux and windows - Troubleshoot and resolve various Oracle connectivity problems. - Provide network troubleshooting and administrative support for the development staff - Analyzing the Tables and Indexes on performance base regularly - Performed hot and cold backup and recovery using RMAN and Linux Scripts - Export and Import of database objects to copy from one database to another database. - Performed bulk load to database using sql loader - Improved vital processing jobs by reducing process duration by 60% - Regular Monitoring Alert log Files and trace files on Day to Day Basis - Experienced with SRVCTL, OCR, Voting Disk of 11g RAC - Created and maintain Oracle DataGuard configuration, also Managed Data Guard using Data Guard broker. - Implemented Dataguard(Standby) for high availability disaster recovery purpose - Experience in performance tuning using cost based optimization (CBO) - Performed database tuning using explain plan and enterprise manager - Implemented disaster recovery system, using RMAN and custom written shell scripts. - Optimized database by monitoring the statspack, AWR and ADDM report generated from snapshots taken at peak business. - Rebuilding indexes when needed to avoid fragmentation and improve performance, monitoring index usage and removing unused indexes. Education Bachelor's of Arts University of Maryland-Baltimore County Certification Information technology Boltos Solutions Institute Skills Nessus Vulnerability Scanner, IBM,

IBM/BigFix, Oracle Database 10g; 11g; 12c, Microsoft SQL, LINUX/UNIX OS, Mac, Microsoft Windows ,Excel, Word, PowerPoint, Access, People Soft, MS Project, MS Visio, and VMware, Oracle virtual box, CSAM, Accellion/WatchDox secure file solution, Microsoft SQL Server, Management Studio, Xactimate, NextGen, Oracle 10g, Oracle 11g, Oracle 12c, Rac Database, DataGuard, People Soft, Database, ASM, Enterprise Manager, Security, Quality Control, Disaster Recovery, MySQL, PL/SQL (4 years), Apple, Nist, Information Security, Cyber Security, Siem Certifications/Licenses OCA Oracle Database 11g Certified Associates Present Oracle Database 11g SQL Fundamentals I Present CAP Certified Authorization Professional CISSP In Progress OCP Oracle Database 11g Certified Professional Security+ Additional Information Professional Summary

Assessment and Authorization (A&A) Certification and Accreditation (C&A) IT Security Compliance Vulnerability Assessment Vulnerability Scanning Database Administration Information gathering Information Assurance Risk Assessment Systems Development Life Cycle Technical Writing Project Management and Support Project evaluations Analysis and reporting Proficient in Oracle 10g, 11g and 12c Database Administration Proficient in Enterprise Manager Proficient in RMAN, Backup and Recovery Proficient in Database Migration, Upgrade and Patch Application Performance Tuning Real Application Clusters Data Guard Administration A self-motivated, responsible and reliable team player with a set of strong technical skills Strong in solving problems of diverse scope where technical analysis and evaluation is required Results-driven IT personnel with skills in team building and problem-solving with an established reputation for effectively working with diverse groups of people and adaptability to changing environments Professional Certification

Name: Dana Graham

Email: millerbrandon@example.org

Phone: 273.240.3661x86143