Cyber Security Manager Cyber Security Manager Cyber Security Governance & Compliance Professional The Colony, TX To pursue my career in Information Security with an established organization. Work Experience Cyber Security Manager CBRE - Richardson, TX April 2019 to July 2019 Cyber Security manager responsible for cyber security governance and compliance activities at CBRE. Draft & publish security policies & procedures Conducted security assessments & reviews on third-party vendors to ensure compliance with CBRE policies as well as regulatory requirements Reviewed processes with business organizations to determine any security gaps and identify proper controls to mitigate risk Interviewed candidates for open positions within the department IT Security Compliance Analyst Texas instruments - Richardson, TX August 2015 to April 2019 IT Security compliance liaison for TI Mexico site. This requires conducting site visits & providing security awareness training and providing security risk analysis for projects in Mexico. All this is provided in Spanish. Craft and communicate updated, effective Cybersecurity Policies and procedures based on ISO 270001:2013 framework Perform and document security analysis of Risk Acceptance and other requests Effectively utilize the Archer Policy and Compliance Management tool. This includes administration and development of the Archer GRC tool Promote security compliance within the organization through policy development, formal and informal communication, and security assessments Engage and build relationships with other groups within Texas Instruments, including auditors, business teams, vendors, customers, and partners Develop, monitor and communicate effective compliance metrics Evaluate new threats and vulnerabilities to determine impact to information resources and what countermeasures should be deployed both technical and procedural Responsible for the creation of a formalized Third party review process. This includes coordinating with key stakeholders, develop and map process flows, assign ownership for key controls in the process & implement in our GRC tool Perform on-site third party security assessments for our vendors in Mexico. This required reviewing security controls & processes for vendors are adequate according to TI standards as listed in contracts requirements. Senior Security Compliance Analyst Nationstar Mortgage - Irving, TX June 2014 to July 2015 Responsible for evaluating vendors to ensure they are in compliance with all Nationstar information

security requirements, reviewing contracts for security concerns, ensuring new contracts have appropriate information security verbiage and creating monitoring and remediation processes; this includes reviewing all vendors (U.S. offshore, nearshore) which require information security review for Nationstar Mortgage and its subsidiaries (Solutionstar, Greenlight) and provide a risk rating for services to be provided by vendor Overhauled the vendor information security review process by establishing a security review process model, defining scopes of review, creating information security questionnaires, agreeing to service level agreements and creating a list of required documentation from vendors; as a result, the process is streamlined and vendors are reviewed and process efficiently Re-evaluate processes to stay current with the industry standards and frameworks (ISO27001, AICPA TSP, NIST, etc) and requirements (GLBA, SOX, SSAE16, etc) and relevant with the third party threat environment Provide guidance and training to vendor management teams and business organizations on key information security governance and processes for reduction of third party risk Drive the reporting and remediation of information security governance violations Develop mitigation and remediation plans and overall risk assessments as part of the security exception process Information Technology Auditor University of Texas at El Paso - El Paso, TX November 2012 to June 2014 Develop, administer, conduct, and responsible for all information technology / information security audit activity for the entire university. My scope of audit responsibility consists of performing audits on the UTEP network to ensure policies and controls are applied and in compliance with TAC 202, PCI, and other information security standards (SANS Top 20, NIST, etc.) Develop all audit programs and procedures. Responsible for all information systems audit activity which includes coordinating, planning, gathering information, analysis, summarizing results, identifying problem areas, and recommending solutions to problems Conduct formal presentations to management officials and provide advice and recommendations on information systems security issues System Administrator for the Teammate Audit Management System Conduct training on information security principles and policies to UTEP staff and students Provide I.T. and information security audit training to the IIA El Paso chapter I.T. Support / Internet Sales Consultant Casa Nissan - El Paso, TX August 2011 to October 2012 Install, configure Layer 2 and

Layer 3 network devices for Casa Nissan. Responsible for establishing wireless network connectivity for sales personnel use. This resulted in sales personnel being able to enter client data from mobile devices (i.e. iPads, tablets, laptops, smart phones) Sales Consultant responsible for establishing customer relations with potential, current, and previous customers Systems Administrator EPIC Technologies - El Paso, TX April 2011 to August 2011 Administrator for Network Servers utilizing Windows Server 2003, 2008, Exchange 2003, Blackberry Enterprise Server, WSUS Server Responsible for the day to day administration of all network devices and systems for EPIC Technologies (i.e., server administration, network troubleshooting, switch configuration, access point configuration, cable wiring, etc Install and configure computers, multi-functional devices, and printers to be utilized for network use Coordinated personnel during network security incidents and responded accordingly to minimize downtime loss Project Manager - Safety Engineer Care Fusion - San Diego, CA November 2010 to March 2011 Develop matrices for mapping current hazards to assurance cases based on FDA standards using FMEA procedures Define goals and outline approach and make adjustments within the constraints set to achieve optimum results Coordinate and lead assigned projects ensuring the day-to-day assignments for the Alaris Infusion Pump System Information Assurance Engineer AUSGAR Technologies - San Diego, CA April 2008 to November 2010 Information Assurance Subject Matter Expert for U.S. Navy Experimentation Program, responsible for ensuring organizations (military and commercial), participating in the program are compliant with all security policies and procedures. This includes reviewing all security accreditation packages, planning and execution of security testing events, & providing recommendations for risk reduction and mitigation. As a result of my efforts, all 100 organizations achieved successful accreditation and were able to participate in the program Responsible for the development of all security certification and accreditation documentation being used for the experimentation program. This includes templates and step-by-step instructions Managed a five person certification and accreditation team that is responsible for developing all C&A packages for the experimentation program Vulnerability Management Analyst Sempra Energy, Information Security Department - San Diego, CA October 2007 to March 2008 Perform enterprise vulnerability

management activities within the context of the established vulnerability management process and processes were in alignment with NERC CIP requirements Generate vulnerability assessment reports for directors, managers, and system administrators. Work with other I.T. departments to address vulnerabilities and develop remediation plans with plans of action to fix vulnerabilities in a prompt manner Responsible for the planning, design, coordination, configuration, of network security scanning tools (Rapid 7 Nexpose, Ncircle IP360) Assisted in the risk assessments process by providing technical analysis and conducted vulnerability testing of systems going through risk assessment process Senior Consultant Booz Allen Hamilton - San Diego, CA August 2003 to August 2007 Provide Information Assurance guidance to DoD and U.S. Navy clients in accordance with Information Security policies and procedures. Main emphasis is the development of security requirements and security policies on all projects utilizing multiple National, Department of Defense, and U.S. Navy standards. Security Engineer responsible for ensuring all network devices, servers and PCs are configured correctly and compliant by coordinating with program managers, network engineers and vendors Functional Area Analyst, Level Adecco Technical Services - Fort Huachuca, AZ April 2003 to August 2003 Install, configure Network Operations Center through user-level Defense Message System Review technical documentation and test concepts, execute test events and recommend solutions Senior Technical Support Engineer Raytheon Technical Service Company - Chula Vista, CA September 2002 to April 2003 Analyze, translate and implement security policy into technical requirements Manage overall network security, and customer service support Network Security Officer, Sergeant United States Marine Corps August 1995 to October 2002 Provide leadership for branch, including developing, planning, scheduling, and managing operations and work assignments; staff development programming; motivating and facilitating high degree of technical competence; personnel career, performance and welfare counseling; initiate and approve personnel actions; enforce discipline; resolve grievances. Ensure that Automated Information Systems (AISs) security safeguards and requirement are included in the network design, and that individual nodes of the network comply with these safeguards and requirements prior to interfacing with the network. This included the monitoring of all e-mail, internet, and network devices

for any potential security violation Education Master's in Engineering Technical Management Texas A&M University August 2018 to May 2020 Certified Information Systems Auditor Institute of Internal Auditors January 2013 to October 2014 B.S. in Network Security Coleman University - San Diego, CA December 2010 B.S. in Computer Networks Coleman University - San Diego, CA December 2010 A.S. in Computer Networks Coleman University - San Diego, CA December 2009 Skills audit (2 years), network design (7 years), Security (10+ years), Cyber Security (10+ years), It Security (10+ years), Information Security, Comptia, Compliance (8 years) Military Service Branch: United States Marine Corps Rank: Sergeant Certifications/Licenses Certified Information Systems Auditor (CISA) October 2014 to October 2020 Certification # 14119246 Certified Information Security Manager (CISM) October 2016 to October 2020 Certification #1633663 Additional Information Results-driven Senior Information Security professional with 18 years of information security and auditing experience.   Articulate in analyzing risks and successful at formulating strategic recommendations for problem resolution in order to ensure confidentiality, integrity, and availability of information systems. Broad knowledge of hardware, software, and networking technologies. Able to effectively communicate both orally and in writing to technical and non-technical audiences at all levels in an organization. My areas of expertise include but are not limited to: Information Security Governance / Risk / Compliance   Policy Planning / Implementation   Business Continuity / Disaster Recovery   Vulnerability Management   Certification & Accreditation   Third Party Risk Management   Risk Assessment / Management   I.T. Asset Protection   Access Control   Training & Awareness Professional Competencies   Project Management Interpersonal Relations Instructor   Leadership Asset Management Presentation   Resource Identification & Utilization Staff Supervision Auditing Oral & Written Communication Languages -English, Spanish Research & Documentation Standards, Procedures & Policies Formulation Network Design & Installation Business Process Mapping   Technical Competencies   Hardware: Servers (Dell, Compaq ProLiant, HP), Hubs, Switches (Cisco), PC (Desktops, laptops), other networking equipment   Operating Systems: UNIX, Linux, Windows (Client, Server)   Software/Applications: TeamMate Audit Management System, IDEA, Microsoft Project, Microsoft Exchange; Antivirus (Norton, NOD 32, Trend Micro); Microsoft

Office; Microsoft Visio; Eeye Retina Security Scanning tool; Ncircle IP 360; Rapid7 Nexpose, Spiceworks; NMAP, RSA Archer

Name: Austin Thompson

Email: jessicagreene@example.org

Phone: 840-495-8925x61859