Chief Information Security Officer Chief Information Security Officer Chief Information Security Officer - Atos Orlando, FL I'm seeking a challenging role with within an organization, that's looking for a professional to guide them along the ever-changing technology landscape. I would like to utilize my experience and skills in the information security field to contribute in the efficiency and profitability of an organization. Harnessing this experience to solidify improvements and instill recommendation and or enhancements within an organization overall Security compliance. Work Experience Chief Information Security Officer Atos August 2018 to Present My responsibility is to oversee the overall Service Delivery of the Data Center program for the Texas DIR (Data Center Services) account. My primary focus is to provide account leadership for Governance, Risk, Compliance and Security delivery teams, ensuring that we deliver our services within scope and adhering to Texas Administrative Code Chapter 202 for Information Security Standards. As the primary point of contact for the all Security, Risk and Compliance needs, my requirement and expectation are to ensure that our team protects State of Texas Confidentiality, Integrity and Availability of their Data and Environment. Provide overall account leadership to the service delivery team to develop an effective GRC / Security program, products, and business strategies, implementing resulting solutions to meet contract deliverables Manage and drive remediation efforts related to TAC.202, IRS 1075 and PCI regulations for Texas State Agency environments. Ensure audit-readiness for service delivery as per the contract agreement and that Texas State Agencies meets their yearly regulatory compliance requirements as required. Work collaboratively with individuals/teams to achieve client satisfaction targets. Develop and ensure the implementation of Security Strategies concerning emerging Cyber Treats with all 34 Texas State Agencies ISO's under the program. Participate and represent Atos in Security Delivery meetings; provide monthly overview on the status of the Information Security program with the Office of the CISO in addition to other Executive Stakeholders Use technical knowledge and familiarity with client to identify new opportunities for growth Sr. Information Security Manager Capgemini June 2017 to August 2018 My responsibility is managing Capgemini's Governance Risk and Compliance Security delivery team, ensuring that we deliver our services within the Carnival's Service Level

Agreement. As the primary point of contact for the all Security, Risk and Compliance needs, my requirement and expectation are to ensure that our team protects Carnival's Confidentiality, Integrity and Availability of their Data and Environment. Provide overall account leadership to the service delivery team to develop an effective GRC / Security program, products, and business strategies, implementing resulting solutions to meet contract deliverables Ensure audit-readiness for service delivery as per the contract agreement and that Carnival meets their yearly Sarbanes-Oxley (SOX) controls and Payment Card Industry (PCI) attestation and other privacy and/or regulatory compliance requirements as required. Manage and drive remediation efforts related to SOX, PCI for Carnivals environment. Work collaboratively with individuals/teams to achieve client satisfaction targets. Develop and ensure the implementation of Security Strategies concerning emerging Cyber Treats. Participate and represent Carnival Security Delivery meetings; provide monthly overview on the status of the Information Security program with the Office of the CISO in addition to other Executive Stakeholders Use technical knowledge and familiarity with client to identify new opportunities for growth Involve in contract solutions. Position myself as a trusted security advisor and while promoting new solutions to the Carnivals Global Security teams. Responsible for defining and owning the Service/Quality Improvement plan Sr. Security Manager, Data Privacy and Loss Prevention Beacon Hill Staffing July 2016 to May 2017 Responsibility includes management of the Data Privacy and Loss Prevention Program for Client Toyota Financial Services, supporting TFS corporate business services, including management of the Security Architecture for Data Loss Prevention (DLP), Data Discovery, Email Prevent, Mobile DLP, Risk and Compliance program and Cloud Access Security Broker (CASB). Lead a team of offshore resources providing standards, guidelines and procedures to follow during maintenance and operations, formulate and define technical scope and objectives of the DLP program Managed the TFS Cloud Access Security Broker (CASB) framework roadmap and implementation project. Ensure that DLP/CASB program deliverables are aligned with SOX, Payment Card Industry (PCI) and other privacy and/or regulatory compliance requirements. Collaborate/participate with internal/external auditors to conduct Security Risk and Compliance assessments, SOX and Payment

Card Industry (PCI) audits, presenting results to senior management. Design and maintain policies, response rules and data identifiers for effective discovery of data at rest and data in motion and align with the cyber- security initiative to deliver 24x7 Data Loss Prevention functions Sr. Manager IT Nuclear Security and Compliance Program Energy Future Holdings July 2014 to July 2016 Responsibility includes management of the Cyber Nuclear Program; serve as the single-point of contact for the Cyber Security Initiatives within the Nuclear Power Generation Facility. Focus on Information Security and compliance initiatives concerning NRC 10 CFR 73.54/73.77, NEI 08-09/13-10, NERC CIP Version 5. Manage and coordinate activities for multiple Information Security initiatives both at corporate and nuclear facility. Formulate and define technical scope and objectives of the program. Sr. Security Project Manager - Contractor Bank United February 2014 to July 2014 Focus on Information Security and GRC initiatives from a Technical SME and Project Management perspective. Formulate and define technical scope and objectives of projects. Identifying and scheduling project deliverables, milestones, and required tasks. Project Manage vendor selection and "Go Live" and testing of Various Security tools and current Identity Access Management Platform upgrade. Develop project plan that in line with business objectives and deliver to management and or customers and review project plans outlining goals, time frame, funding limitations, staffing requirements, allotment of resources, scheduling, and identification of risks, contingency plans, allocation of available resources and procedures for accomplishing project. Work with the Information Security team to develop standard infrastructure build requirements for new and existing IT/ Security Platforms Deliver Information Security's standard infrastructure build requirements to appropriate parties, monitor implementation of standard, and coordinate approval for any exemptions from standards and procedures for project reporting and documentation. Work with appropriate stakeholders to Define, Identify and schedule project deliverables, milestones, and required tasks. Coordinate and respond to requests for changes from original specifications. Director of Strategic Services Fishnet Security October 2013 to February 2014 Focus on developing business opportunities by expanding existing and growing profitable, long-term relationships with clients. Ensure positive marketplace perception of Fishnet Security within assigned territory

Provide support to achieve revenue generation targets and business growth of MSS revenue based upon defined GP budget targets.   Support and educate all sales resources in identifying and positioning Managed Security Services   Understand and consult on client's business objectives and goals pertaining to security, compliance and governance including ITIL, SOX, SSAE16, PCI-DSS 2.0, HIPAA, ISO 27001 standards and requirements.   Post-meeting follow-up with appropriate customer contacts to confirm that Fishnet Security's understanding, strategy, and direction are in line with client service proposal expectations. Director IT Security Operations (Global) Trapezoid Digital Security October 2011 to October 2013 Reporting to the Chief Technology Officer, My principal responsibility is for the Global Managed Security and Professional services.   Responsibility includes evaluating and managing new initiatives, and business opportunities, overseeing market analysis, while monitoring competitive activity and identifying customer needs.   Developing annual IT/Operations department's budget, assisting sales organization goals are achieved from operational compliance.   Provide leadership in planning, designing, and implementing business plans with information technology strategies.   Build internal business policy and objectives pertaining to compliance and governance referencing ISO 27001, PCI-DSS 2.0, SAS70, SOX, SSAE16, standards and requirements.   Areas of expertise is on developing solutions as they relate to the future business environment and helping conceptualize Managed Services as key and valuable to client's future growth model.   Partnering with business leaders create, manage & communicate long range IT strategies and supporting roadmaps for Global Operations. Ensure alignment with Global & SBU managers to deliver consistent, innovative solutions for business process visions.   Envision, develop & manage core IT governance processes for ensuring Strategic IT / business alignment, managing IT investments, and delivering IT projects & services for Global Operations. Lead development and enhancement of policies and procedures required Cyber Security Initiatives August 2009 to October 2013 Responsibility includes management of the Cyber Nuclear Program; serve as the single-point of contact for the Cyber Security Initiatives within the Nuclear Power Generation Facility. Focus on Information Security and compliance initiatives concerning NRC 10 CFR 73.54/73.77, NEI 08-09/13-10, NERC CIP Version 5.

Manage and coordinate activities for multiple Information Security initiatives both at corporate and nuclear facility. Formulate and define technical scope and objectives of the program. Primary contact for incident response for internal and external clients to report any security event or incidents including server compromise, corporate espionage, inappropriate employee internet or email usage, or breaches of confidentiality. Responsible for documenting all evidence obtained from computer forensic investigations and implementing the appropriate business continuity plans. Lead development and enhancement of policies and procedures required to implement regulatory required cyber security programs within (NEI 08-09/13-10 RG 5.71 and NERC CIP Version 5) for Milestone 8. Perform Security Risk and Compliance assessments as required by the NRC/FERC/NERC, SOX and Payment Card Industry (PCI) programs. Ensure audit-readiness for service delivery as per the internal requirements and that EFH meets our yearly Sarbanes-Oxley (SOX) controls and Payment Card Industry (PCI) attestation and other privacy and/or regulatory compliance requirements as required. Manage and drive remediation efforts related to SOX, PCI for EFH Corporate, Luminant and TXU environment. Ensure that program deliverables are aligned with SOX, Payment Card Industry (PCI), and Nuclear Regulatory Commission (NRC), NACHA, and other privacy and/or regulatory compliance requirements Manage program intersections and dependencies with stakeholder groups across IT and the company. Insure proper project communication across the project team, stakeholders, and across the organization Interact with service providers and vendors, 3rd parties and Manage vendor selection of Various Security Drive the evaluation of technical, operational and management controls for Critical Digital Assets per NEI 08-09 and ensure that local plant guideline/procedures adequately align with Milestone 8 Evaluate Critical Digital Assets (CDAs) for compliance with cybersecurity policies and review configurations of CDA's against the NIST cyber security controls and identify gaps, create remediation plans to control any security gaps identified in the CDA assessments Direct a team that drives the identification of Cyber/System Vulnerabilities provide a solution or enhancement patch these devices Responsible for updates/changes to the local Plant Cyber Security guidelines/procedures Participate in weekly and biweekly NITSL and Utilities Service Alliance (USA) Cyber project team's calls Manager Secure Engineering (Global) A Verizon Company June 2008 to October 2011 Reporting to the VP of Security Engineering, My principal responsibility is for the Global Managed Security Services. Architected & Implemented Managed Security Services for 9 countries and over 200 clients. Provide leadership and vision in development, acquisition, implementation, and support of clients managed services offering. Build and develop Security organizational processes/procedures to support strategic direction and clients and business needs. Directed 4 Global Security mission-critical Operations Centers across North America, Latin America and EMEA. Oversaw 75 Security Engineers and Analyst Ensure creation and implementation of cost-effective systems and efficient computer operations to meet current and future decision-making requirements. Functioned as member of Terremark's IT Security Council and Terremark's Compliance Team and in addition participated in Global Compliance and Governance initiatives around ISO/SOX, Fed-Ramp, PCI-DSS and NIST activities in our 7 Data Center Facilities. Senior Security Manager (Global) Electronic Data Systems (EDS) October 2003 to June 2008 Primary contact for incident response for internal and external clients to report any security event or incidents including server compromise, corporate espionage, inappropriate employee internet or email usage, or breaches of confidentiality. Responsible for documenting all evidence obtained from computer forensic investigations and implementing the appropriate business continuity plans. Investigate, diagnose, resolve, and remediate IDS, ISS, McAfee, Surefire, and firewall alerts/vulnerabilities. These alerts mainly pertain to machines that have Windows 2000/2003, Unix, Solaris, and Linux operating systems. Use various software tools to analyze client networks and devices to assess and remediate security risks. Report those events to system administrators, and provide/assist with establishing a solution to eliminate the vulnerabilities and bring the systems to the industry standard level of security. Intimate working knowledge of TCP/IP, IPSec, NAT, VPN, WINS, network architecture, DNS, IIS, DHCP, IDS, and ISS. Ability to communicate effectively, orally and written, with various internal client and government based entities regarding investigations. Consult within my assigned clients for building internal business policies and objectives pertaining to compliance and governance referencing PCI, SAS70, Sarbanes-Oxley (SOX), GLBA standards and requirements. Responsible for creating documentation for training and support of new and existing clients. Also responsible for creating documentation for new technologies. Developed training for the regional security center in Saragossa, Spain which required dealing with European privacy laws and regulations. Subject Matter Expert for EDS' Enterprise Security Event Management offering and IDS. Responsible for IDS sensor tuning and alert filtering. GCIRT (Global Computer Incident Response Team). Setup, trained, developed documentation, performed audits on internal case documentation, and responsible for the day-to-day activities for assigned clients. Senior Systems Analyst (S. Florida, Latin America & Caribbean) AMR/Sabre Travel Network/ Electronic Data Systems November 1999 to October 2003 LAN Administrator / Systems Integrator (South Florida & Caribbean District.) Siemens Building Technologies June 1997 to November 1999 Network Analyst (South Florida) Henry Lee Company January 1995 to June 1997 Systems Technician P/T Tandy Corporation March 1994 to April 1997 Lead Computer Operator Jan - Bell Marketing November 1993 to February 1995 Computer Specialist I Comcast Cable May 1992 to October 1993 Lead Computer Operator Amerifirst Bank / Washington Mutual Bank February 1989 to October 1992 Education Bachelor's in Management Information Systems Florida International University - Miami, FL August 2001 to May 2007 Skills Information Security, It Security, Hippa, Cissp, Compliance, Nist, SOX

Name: Melissa Butler DVM

Email: kortiz@example.net

Phone: +1-461-453-7202x78689