Information Security & Compliance Analyst Information Security & Compliance Analyst Information Security & Compliance Analyst - LVVWD North Las Vegas, NV Authorized to work in the US for any employer Work Experience Information Security & Compliance Analyst Las Vegas Valley Water District - Las Vegas, NV August 2018 to Present Conducted control reviews, Gap Analysis, Constructed POA&M ensuring the findings are documented, classified and addresses appropriate action. Ensured the adherence to operational effectiveness with Payment Card Industries Data Security Standards (PCI DSS) and ISO 27000 as well as internal policies and procedures. Assisted the evolution of security policies, procedures and baselines as part of on-going compliance efforts taking into considerations SANS 20 critical controls, ISO and FedRamp.   Created multiple non-production domains for testing/evaluating security posture. Taught penetration testing course to IT Security Division which resulted in identifying insecure configurations on our production domain and their remediation.   Configured virtualized domain for domain task automation via VSTS and Powershell scripting to enhance workflows, enforce change-management and deployment governance in all aspects of Domain Administration (ADUC/GPMC/PKI).   Taught a period of instruction to ISC on how to dump volatile memory and transform the data to useful intel. Architected comprehensive Digital Forensic Incident Response SOP and the automated in-house powershell DFIR toolkit with Auditing module for remote and automated threat hunting.   Interact with end-users concerning malware, spam, vulnerabilities and other cybersecurity issues. Introduced Vulnerability Time & Exposure Metrics to evaluate security of 3rd Party Library vendors (pre-Fortify).   Architected and performed annual end-user security trianing, including best practices as technologies mature.   Responsible for maintenance of Information Security Systems for Risk Assessments, and security compliance requirements.   SIEM experience and monitors security alerts and feeds from threat intelligence sources MS-ISAC, IBM, SANS, etc.Communicate directly with the IT customer regarding security issues to resolve tickets and report to Director.   Tailored Security Development Life Cycle to make it a streamlined approach for provisioning and deprovisioning systems and service accounts, EOL, EOS warranty, roles and responsibilities. Managed all System Security Authorization Agreements.   Aided all divisions in Continuity of

Operations plans with regard to information security. Installed a Public Key Infrastructure, Policy and SOP and taught this to the Information Technology Department. Participated in the migration of on-prem ADFS tenant to Azure (off-prem cloud AD tenant). Assisted scripting the GPO via powershell that created a scheduled task to migrate mailboxes between tenants and deleted old OST files. Installed and taught Just In Time Administration, Just Enough Administration and Local Administrator Password Solution (JIT, JEA and LAPS) for governance of privilege auditing, and access control for on premises and cloud based applications. Profiecient with powershell management of ADUC, GPMC, and modular scripting, QRADAR, InsightVM (Nessus), Slingshot, Caine, Remnux and Kali Linux distributions, Hashcat, John The Ripper, Metasploit, Wireshark, Packet Squirrel, Bluecoat, Fireeye NX, FTKImager, Volatility, Rekall, NetMRI, Solar Winds NTM, WhatsUpGold, Responder, Social Engineering Toolkit, NMAP, Visual Studio. Scrum Master expertly performed stakeholder management. Log Management Expert. Director of IT & InfoSec Manager USMC - Cherry Point, NC May 2013 to June 2018 Highly skilled with hardware cryptography (EKMS, PKI, SKL, TACLANE, PRC, USB-ENTR, KSV-21B, STE, etc). Designed, communicated, and enforced Information System Security Policies including secure network design, information exchange requirements, disaster recovery plans, and emergency destruction plans. Accounted for 4315 classified artifacts and 50+ employees while embarking and deploying to disparate locations. Internal auditing cybersecurity regulatory compliance lead, 18 inspections, 100% compliance with regulatory requirements. Tracked overall execution of personnel and system-level POA&Ms in a dynamic disparate environments. Designed detailed self-inspection programs resulting in 25 3rd party audits 100% regulation compliance. Provided quarterly information system security awareness training to 120 users. DoD Certification and Accreditation (C&A)/Authority to Operate (ATO) (RMF/DIACAP) practitioner. Installed, configured, and sustained systems throught Security Development Life Cycle. Created technical training standards, performed instruction, evaluated practical application, tracked skills of 50 employees. Coordinated and adhered to Certification and Accreditation of IT systems with Security Teams like Joint Chiefs of Staff, Air Force, USMC C4, and Cherry Point Security Division/G6. Tested Command and Control

Systems including but not limited to CAC2S, Air Defense Systems Integrator (ADSI) and Communications Data Link System (CDLS). Installed Theater Battle Management Core System to be used as Cloud based solution for remote Air Tasking Order dissemination and management which has been used in operations and training around the world. Lead this installation and provisioning from its inception through implementation in an Agile manner. Directed, organized, and evaluated the workflow of 150 employees and equipment totaling 12 Million Dollars. Installed, configured, and sustained systems throught Security Development Life Cycle. Managed and configured Organizations Sharepoint site. Created technical training standards, performed instruction, evaluated practical application, tracked skills of 50 employees. Marine Recruiter U.S. Marine Corps - Chicago, IL January 2010 to May 2013 Worked independently, performed customer service, displayed advanced communication and presentation skills. Data Systems Technician USMC April 2004 to January 2010 Tier I Helpdesk technician for Cisco, Solaris, Unix, Linux and Microsoft information computing systems. In depth hands-on skills configuring VLAN, ACL, OSPF, EIGRP, BGP, SNMP, SMB, SSL, DNS, DHCP, etc. Education Bachelor's in Computer science networking and security Park University - Parkville, MO August 2013 to March 2019 Skills Cissp, Compliance, Hippa, Nist, It Security, Information Security, Cobit Links https://linkedin.com/in/garland-brown-cissp-csm-b9b7b6123 Military Service Branch: United States Marine Corps Rank: E7, GUNNERY SERGEANT Certifications/Licenses CISSP April 2017 to April 2020 Certified ScrumMaster (CSM) May 2019 to May 2021

Name: Brian Gibson

Email: samanthagonzalez@example.com

Phone: (858)942-5264x8653