IT Specialist (InfoSec) IT Specialist (InfoSec) IT Specialist (InfoSec) Jacksonville, AR To contribute my skills and experience as an Information Security Analyst into enhancing the rate of cyber incidence response and mitigation into our existing critical infrastructures. Authorized to work in the US for any employer Work Experience IT Specialist (InfoSec) JACKSONVILLE NORTH PULASKI SCHOOL DISTRICT - Jacksonville, AR August 2017 to January 2018 Monitors and troubleshoots the security of district critical systems and changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigate and report on noted abnormalities. Security tools used: Fire-eye, Splunk, Secure-works, Carbon black, OSSEC, IBM Q radar Monitors security events from servers, firewalls and intrusion detection system (IDS) for potential security breaches or violations of policy in the entire school district. Identified vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls. Assisted in major upgrade and optimization of the districts core network infrastructure for optimal performance, scalability, resiliency and reliability. Provides and maintains network connectivity and services to the entire school district. Install and maintain classrooms instructional technology facilities for both teacher and student to enhance learning. Creates user accounts and managed access control of systems and Network applications. Maintains & secures inventory database and provide support for networks, computer, video and audio conferencing systems . Install and implement new programs, modules, servers, hardware, network equipment when necessary to upgrade, improve resources or increase compatibility. IT Graduate Assistant ARKANSAS TECH UNIVERSITY - Russellville, AR August 2016 to July 2017 Security tools used: Checkpoint, OSSEC, SolarWind Log, Event Manager & Carbon Black. Assist in installation and troubleshooting of campus physical security systems and incidence response applications for classroom instruction technology. Monitor, operate, manage, troubleshoot, and restore service to terminal service clients, PCs, or notebooks with authorized access to network. Assist network support engineers & technicians in installing and optimizing the university's enterprise network infrastructure for multiple classrooms and student support. Assist in the development of strategies for attaining greater compliance and reducing risks. Assist in the design, implementation and audit of change control

and release management as defined through standard Operating procedures. Prepared detailed IT security practices and procedures for technical processes. Assist in the Development and operation of incidence response applications using Internet of Things (IoT) sensors empowered devices to Identify, report, and patch vulnerabilities in the university's critical infrastructure. Conduct research in writing incident response report using the RSA Archer & VERIS Incident report. Information Security & Systems Analyst BIOWAYLLIS INC - Lagos, NG April 2014 to November 2015 Conducted incident prevention, detection/analysis, containment, eradication and aid recovery across IT systems which has increased customer's data safety by 98%. Assist in Training staffs on security awareness, policy and compliance. Proactively assigned resources to meet workflow needs. Security tools used: Splunk, Alien Vault, Fire-eye, Nessus and IBM Q radar Identified vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls. Educated business unit managers, IT development team, and the user community about risks and security controls. Enacting security needs, enhancement and security purchases to security-oriented organizations such as banks, and insurance firms Analyzed security incidents and presented a quarterly report to the CIO. Evaluate customer and product requirements to develop total systems solutions within project timelines and cost constraints. Enacted the use of security metrics to mitigate vulnerability by analyzing historical threats, addressing risks/gaps/violations and implementing improved protocols on all existing systems. Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools. Ensure proper operation of security database records to make sure that all staffs keep up with, data confidentiality, integrity, availability and security logging, and check-ups. Installing firewalls, data encryption tools and other security hardware. Monitored events, responded to incidents and reported findings. Communication security systems Technician Federal Airport Authority of Nigeria - Lagos, NG March 2012 to February 2013 FAAN) Murtala Muhammed int'l Airport Ikeja, Lagos, Nigeria. March 15th, 2012 - February, 2nd, 2013 Communication security systems Technician Assisted in security operations for both physical and cloud infrastructures by acting as the main

point of referenced for investigating, responding and resolving security-related issues. Develop threat and vulnerability management policies and manage SIEM applications using OSSEC and BRO Security tools used: Splunk, OSSEC, LogRhythm, Nessus & Symantec. Ensure proper operation of security data base records to make sure that all staffs keep up with, data confidentiality, integrity, availability and security logging and check-ups. Creates testing, and implementing network disaster recovery trainings section to other staffs which helps increases and strengthens the company's manpower & skills in enterprise network and data recovery. Administer IP video management services for IP video record storage and keep records of security check-ups on all surveillance systems Installing firewalls, data encryption tools and other security hardware to detect and countermeasure every form of threat both internally & externally. Monitors security-events from servers, firewalls, intrusion detection system (IDS) and access control for potential security breaches or violations of policy. Conduct technical presentations on end-user IT security training and awareness, security policies and guidelines. Performs weekly software simulations to Check and monitors physical security vulnerabilities applicable to information systems and Gives weekly mitigation recommendations to other departmental systems owners and tracks progress in applying cyber mitigation. Education Masters in Emergency Management & Homeland Security Arkansas Tech university - Russellville, AR January 2017 to December 2017 Bachelors in Applied Physics Oduduwa University April 2011 to November 2013 Associates in Electronics & Computer Engineering Lagos State University - Lagos, NG September 2007 to October 2009 Skills SECURITY (3 years), SPLUNK (2 years), ENCRYPTION (2 years), NESSUS (2 years), SIEM (2 years) Additional Information Bringing High performances into the quality of Network & information infrastructure security by ensuring technical security planning, testing, verification and risk analysis. Also, the ability to deploy and monitoring risk management, compliance, and information security programs while functioning as an incidence response team catalyst KEY COMPETENCIES: Monitoring Monitor the security of critical systems (e.g., e-mail servers, database servers, web servers, etc.) and changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigate and report on noted irregularities. Conduct network

vulnerability assessments using tools to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures. Ensure organizational compliance with CFCU information security programs. Manage SIEM infrastructure. Conduct routine social engineering tests and clean-desk audits. Investigate potential or actual security violations or incidents in an effort to identify issues and areas that require new security measures or policy changes. Strategy Development Research new developments in IT security in order to recommend, develop and implement new security policies, standards, procedures and operating doctrines across a major global enterprise. Define, establish and manage security risk metrics and track effectiveness. Coordinate with third parties to perform vulnerability tests and create security authorization agreements and standards. The ability to balance risk mitigation with business needs. Disaster Recovery Collaborate with business units to determine continuity requirements. Conduct business impact analysis for vital functions; document recovery priorities of the key processes, applications, and data. Establish disaster recovery testing methodology. Plan and coordinate the testing of recovery support and business resumption procedures while ensuring the recovery and restoration of key IT resources and data and the resumption of critical systems within the desired timeframe. Technical Expertise Platforms: Windows OS 7,8,10 & Mac OSX; Windows Server 2008, 2012, Ubuntu, Linux Debian, Kali, SElinux & Cubes; Android OS. Networking: LAN/WAN Administration, Cisco 2500/2600 series routers, Cisco switches 1900/2950/3550, HPE, Cisco ASA Router PPP, Wireshark, TCP/IP, UDP, DHCP, DNS, LDAP, G-suites, FTP, POP, IMAP, SMTP, SYSLOG, NTP, SNMP, BGP, EIGRP, OSPF, RIPv2, TELNET, IP-table, snort, access-list, ATM, SSH, SNMP, PPP, ICMP, ARP, VPN, IP-SEC, AAA, MS-CHAP, PAP, RADIUS, PPP, HTTPS, SSH, DMZ, VLAN, Frame relay, ADS, IIS-7, WDM, Wire shark, Spice works, PRTG, and Winpcap. Security Tools: Sandboxing, Virtual box & VMware compartmentalization, Malware & Vulnerability analysis tools, Disk encryption, Security Tokens, Endpoint protection, Armitage, Packet sniffers, Metasploit Framework, net-expose, Nessus, Burpsuite, Cain & Abel, Acunetix, John the Reaper, Reaver, Zed attack proxy, Retina, Avigilon, FireEye, Canvas, SET, OSSIM, OWASP, OSSEC, Splunk, Q Radar, Fire eye, RSA Ecat, RSA Archer, Carbon Black, LogRhythm, ESM, Sift

Workstation, SolarWind Event Manager, EPO, Snort, PfSense, OS Query, Nmap, SQL Ninja, Shodan, Nagios, Beef, Maltego, Recuva, Mini-tool partition recovery, LOIC, Lynis, IP-tables, snort, & access-list. Security Compliance Frameworks: ISO27001, NIST, Cyber Kill chain, HIPAA, & CIS, PCI, ISO & GPDR. Languages: Bash Scripting, JavaScript, CSS and HTML 5.

Name: Dennis Romero

Email: anna04@example.net

Phone: 2087473546