Cyber Intrusion Detection Analyst Cyber Intrusion Detection Analyst Cyber Intrusion Detection Analyst - FBI Laurel, MD Work Experience Cyber Intrusion Detection Analyst FBI November 2015 to Present Monitoring and analysis of alerts triggered on sensors to determine malicious activities and unwanted traffic and initiating and monitoring requests to address relevant vulnerabilities and other security event data sources on a 24x7x365 basis. Deploy, troubleshoot, and maintain network-based vulnerability scanners at subscriber sites to ensure appropriate coverage of scanning services. Perform analysis related to the detection, characterization, monitoring and warning of suspected unauthorized network activity and relationships that may pose a threat to our networks. Reviews reported tips and leads for threat information and situational awareness, including determining Location, activity, severity and reporting trends. Managing systems security monitoring, IDS, IPS and computer incident handling and response capability, in managing a 24x7x365 systems security monitoring operations Conducts open-source and classified research on emerging/trending threats and vulnerabilities Pull Common Vulnerabilities and Exposures (CVE) data bases from NIST webpage to update our own vulnerability patch management requirement software. Create our own vulnerabilities patch management for all FBI FISA customer. Conducts cyber intelligence analysis utilizing open-source and classified research on emerging/trending threats and vulnerabilities and importing information into databases. Cross checking malicious IPs and domains to determine if they have been blacklisted and keeping a daily log of such domains for future analysis. Selected to be part of additional teams such as Advanced Threat and COOP (continuity of operations planning) during essential missions. Scanned for rogue (unknown) hosts on the network, which includes unauthorized network peripherals such as printers, laptops, PDAs, and taking them of the network for compliance and proper identification Cyber defense analyst Kingfisher Systems, Department of education, INC July 2014 to November 2015 Cyber Defense Analyst, provide first/second level IDS monitoring, analysis and incident response to information security alerts events. Analyze network traffic and IDS alerts to assess, prioritize and differentiate between potential intrusion attempts and false alarms. Compose and send alert notifications. Recommend IDS filters to eliminate false positives Plan, organize, and

support Vulnerability Management activities. Tasks include vulnerability scanning, scan results analysis, vulnerability tracking, and Independent Validation and Verification (IV&V) activities. Report all incident and severity levels following US-CERT guidelines. Police officer Anne arundel police department - Annapolis, MD May 2013 to July 2014 As a Law Enforcement officer my duties are to: * Protects life and property through the enforcement of laws & regulations; patrols assigned areas * Responds to calls for police service * preliminary & follow-up criminal and traffic investigations * Conducts interviews * Prepares written reports and field notes of investigations and patrol activities * Arrest and processes criminals * Testifies in court * Emergency duties required during adverse weather conditions * Ability to exercise judgment in determining when to use force and to what degree * Operate a law enforcement vehicle under emergency conditions day or night * Comprehending legal documents including citations, affidavits and warrants but not limited to. * Commanding emergency personnel at accident emergencies and disasters Junior Cyber Defense Analysts BATTELLE THE BUSINESS OF INNOVATION - Aberdeen, MD February 2012 to May 2013 Monitors Battelle's nationwide computer and communications networks and provides analysis and remediation capabilities to the business, scientific, research, and special project networks. Work with CIO staff members, corporate managers, and other organization security staff as needed to understand network situations, provide targeted analysis of events and outcomes, and redress exploitation attempts and misconfiguration errors. * Analyze incident, prepare reports to describe the event and suggest ways to counter it. * Monitor and assess network traffic and communications across Battelle's nationwide network using commercial and custom tools. * Have a great understanding of a heterogeneous mix of infrastructure and endpoint equipment how vendor diverse products interoperate. Network Administrator Supervisor United States navy, USS ABRAHAM LINCOLN - Everett, WA November 2009 to November 2011 Responsible for network policy development and execution including wide-scale disk quota management, software update scheduling and verification, and SharePoint administration. Overall subject matter expert consulted for all upper-level network issues and proposals. Found issues with established baseline security template and submitted to higher authority for correction. * Collated

baseline network documentation and system administrator guides into a centralized location to be used as the first line of troubleshooting for network issues. * Developed VMware VI best practices for network administrators and put in place standard operating procedures for its use. Help Desk Technician United States Navy US FORCES AFGHANISTAN, Kabul, Afghanistan - Everett, WA 2009 to 2011 Installed and maintained over 460 NIPR/SIPR workstations, Voice over Internet Protocol (VOIP) and Voice over Secret Internet Protocol (VOSIP) phones. Assisted in the inventory and placing of over 1000 workstations and various peripherals in a 2006 LAN upgrade on board USS Abraham Lincoln. Provided technical support to 3,000+ users and documented trouble call resolutions to increase helpdesk productivity. Oversaw account creation and management within Active Directory. Provided PC hardware repair and acted as warranty liaison when needed. * Successfully worked to completion of over 400 trouble calls. * Assisted in the installation and updating of workstation software. * Collaborated with Senior Network Administrators to identify and mitigate issues caused by software updates. Network Administrator United States navy US FORCES AFGHANISTAN - Kabul, AF January 2009 to July 2009 Sustained all core network services and applications, automated a wide array of administrative tasks through the use of Batch files, VBScript, and Microsoft Task Scheduler. Assisted over 500 users, to include creating web pages, assigning appropriate read/write access and assisting with posting critical information. Cyber Incident Analyst/ Network Administrator United States Navy NAVIOCOM - Fort Meade, MD 2002 to 2009 Drafted 30 national level attack sensing and warning alerts and 10 cyber incident advisories that identified network security vulnerabilities within 13 DoD information systems. Significantly reducing cyber attempts and increased the computer network defense (CND) threat of DoD networks. Education CCNA TESST COLLEGE OF TECHNOLOGY March 2005 Bachelor's Degree in Information's Technology Management American Military University Skills Splunk (1 year), Vlan, Ftp, G3, Http, Netbios, Smtp, Tcp/ip, Cisco, Dns, Exchange, Networking, Sms, Dhcp, Router, Tcp, Telnet, Wins, Sharepoint (6 years), Netapp, Military Additional Information Areas of expertise include: Compose 2.0.3 and 3.5 Administration AD Management & Group Policy Development MSI Package Building & Installation Exchange 2000/2003 Administration Hardware Fault

Isolation System Administrative Troubleshooting Concise Documentation of Issue Resolution Splunk Technical Proficiencies Platforms: Windows 2000/XP, Windows 2000/2003 Server, Cisco IOS, Software: Splunk, SharePoint 3.0, Microsoft SMS 2003, Symantec Antivirus Corporate Edition, Microsoft SQL 2005, MS Office 2007 Suite (Excel, PowerPoint, Word, Access, Outlook), Acronis True Image, Audit Wizard, What's Up Pro, Alcatel X-Vision, OmniVista 2500, Tumbleweed VA Networking: TCP/IP, UDP, WINS, NetBIOS, VLAN, DNS, DHCP, HTTPS, HTTP, FTP, SSH, Telnet, SNMP, SMTP Hardware: IBM 8730 Blade Server T, Netapp FAS270, Netapp FAS2020, HP (DL360, DL380, and ML570 G3 / G4 Servers), Dell PowerVault 775N / PowerEdge 2650 Servers, Cisco 3825 router.

Name: Christine Burns

Email: oshannon@example.org

Phone: 4095520058