Director, Corporate Security Director, Corporate Security Director, Corporate Security Centennial, CO Information Security Professional offering a passion in leadership, architectural support, technical guidance and direction for the protection of information systems. A proven record of success in analysis, design and development of new security initiatives including monitoring effectiveness of the security program for continuous improvement. Ability to participate in the planning and execution of the day to day security operations as well as leading internal and external partners in key initiatives. Risk Management Audit and Assurance Vulnerability Assessment System Design and Architecture Contract Negotiations Project Management Vendor Management Leadership Collaboration Policy Creation ITIL PCI FISMA SOX NIST 800-53 Cisco Imperva Tipping Point Snort Log Rhythm Splunk Python Aruba Linux Qualys Nexpose Core Impact Burp Suite RiskSense Veracode Authorized to work in the US for any employer Work Experience Director, Corporate Security Nelnet, Inc January 2017 to May 2019 Provided oversight and leadership of entire corporate security program including incident response, SOC, pen testing, policy and standards, education, monitoring and logging. Effectively integrated two geographically separate security teams merging and reducing duplicate processes, technical controls and cultures resulting in operational efficiency of roughly $400K in savings. Managed a team in creating a 0-day vulnerability investigative and response process, across multiple business units, reducing the time to identifying impact to the enterprise over 50%. Facilitated replacing commercial IDS sensors with an Open Source solution increasing network traffic visibility resulting in savings of $40K yearly and a one-time savings of $90K. Partnering with CSO, negotiated multiple enterprise agreements to increase functionality and save more than $1 million over three years. Actively managed a budget of over $3 million including salaries and bonuses. Acted as an internal consultant on business and technology projects to ensure appropriate security protection is contemplated, understood, and integrated. Identified and prioritize security initiatives, including to reduce attack surfaces and maintain overall security and data privacy risk at an acceptable level. Develop partnerships with enterprise leadership. Contribute to the professional development of team members, both formally and informally. Represented Information Security on executive

boards and C-Suite. Successfully facilitated vendor partnerships nurturing open and honest working relationships. Directed a team of 3 managers, under which was a total of 17 staff. Manager, Corporate Security Nelnet, Inc - Aurora, CO June 2012 to January 2017 Led a team of security professionals while actively participating in daily security functions. Enhanced enterprise security posture by assessing, selecting and implementing advanced security technology including IDS, firewall monitoring, database monitoring, SIEM, static code analysis and log management tools. Partnered with the CSO on business functions such as budget management, vision and strategy. Managed the replacement of Log Rhythm and SIEM to Splunk and Splunk ES. Performed and directed system, network and web application pen testing. Incident Response Manager coordinating and directing technical efforts and acting as upper management liaison to guide security incidents in a calm, concise manner. Active participant in talent processes of selection, development and management building an enthusiastic, accomplished team. Successfully led a team in a migrating from an outsourced MSSP to a newly created internal SOC saving the company over $300K in reoccurring costs year over year. Led a team to install firewall monitoring using FireMon, that identified over 900 unused firewall rules across 32 firewalls. By eliminating these rules, and instituting a quarterly firewall review process, the company realized a more efficient and secure firewall infrastructure. Partook in $2M budget management. Led the team that installed 6 Snort IDS sensors throughout the environment, enhancing data for SOC monitoring and alerting. Implemented Veracode for static source analysis and partnered with the development teams and leaders to enhancing application code security. Managed a team of 8 highly technical security professionals. Security Analyst, Corporate Security Nelnet, Inc - Aurora, CO April 2010 to June 2012 Managed and administrated security controls including IPS, log management system and vulnerability scanners. Performed enterprise risk analysis, hunting, penetration testing, incident response and forensic duties. Advised management on security best practices reducing risk to the organization. Selected, architected, implemented and administered an enterprise vulnerability scanning tool, Rapid 7's Nexpose, including redesigning the enterprise vulnerability management program to fit the new technology and output. Selected, architected,

implemented and administered Tipping Point IPS border and network protection vastly reducing the risk posture of the enterprise blocking 1M+ malicious events and sources per week. Identification, assessment and prioritization of risk resulting in formal risk assessments to advise stakeholders and management of the probability and impact of threats. Managed MSSP, Secure Works, while monitoring and responding to security alerts. Administered log retention tool, Log Logic, for compliance and contractual requirements. Led the successful initiative that replaced the log management tool Log Logic, with Log Rhythm. Performed penetration testing using open source and commercial tools to identify exposures in system, applications and network infrastructure, while guiding stakeholders on remediation strategies. ? Open Source tools used included but are not limited to: BurpSuite, Kali Linux, Cain and Able, Dirbuster, Foundstone tools, Goolag, Grendal, John the Ripper, MSBA, MaltegoCE, Netcat, Nmap, Nikto, Ophcrack, P0F, PWdump, SQL Inject Me, W3af, WebScarab, WinHTTrack, SQLRecon, XXSme. ? Commercial Tools: Qualys, Eeye Retina, Nessus (commercial feed), Core Impact. Consulted with stakeholders to analyze business processes and to look for ways to reduce risk. Manager, IT Security Frontier Airlines, Inc September 2004 to April 2010 Created and managed the first formal Information Security Department in conjunction with the CIO and Director of Infrastructure. Created policy, procedures and standards to address compliance and assurance requirements. Selected and implemented new technologies to reduce risk throughout a large international enterprise with diverse environments Produced systems standard and hardening guidelines using industry best practices and manufactures recommendations to create deployment standards for Window and Linux systems. Technical lead and project manager on firewall replacement initiative that delivered a standardized firewall, Sidewinder G2's, providing a consistent and secure firewall infrastructure. Oversaw large PCI compliance effort and sub-projects to drive individuals and teams to achieve PCI compliance. Network, System and Application vulnerability and penetration testing using open source and commercial tools. Administration and Management of various security systems. ? IPS/HIDS/IPS: Snort, Tripwire, Tipping Point. ? Firewalls: Juniper, Sidewinder, PIX, ASA. ? Syslog: Log Logic, Snare agents, Kiwi. ? Proxy Servers and Internet Filtering: WebWasher, Surf Control. Implement

24x7x365 security event monitoring and alerting partnering with SecureWorks, Inc. Packet analysis using Tcpdump and Wireshark for troubleshooting, security analysis and forensics Managed budget of over $700,000. Worked in partnership with Internal Audit on IT Audit, Compliance and Assurance programs. System Engineer & Supervisor Frontier Airlines, Inc - Denver, CO September 2000 to September 2004 Responsible for 150+ servers and applications in 7x24x365 operation. Supervised the day-to-day operation of the IT Help Desk and System Engineering staff to achieve 99.99% of mission critical server availability. Successfully migrated 1500+ users, 2000 PC's and 150+ servers from Windows NT4 domain to Windows 2000 AD domain. Effectively upgraded without loss over 2000 NT 4.0 email accounts and public folders to Exchange 2000. Helped with and supervised migration of 35 mission critical servers for data center move resulting in zero down-time. Development of staff to increase their technical knowledge and troubleshooting skills. Assisted in product selection and roll out of AV software to over 2000+ desktops and 150+ servers. Aided in the day to day administration of network routers and switches. Education Bachelor of Science in Aviation Engineer Central Washington University - Ellensburg, WA Skills Information Security (10+ years), It Security (10+ years), Security+ (10+ years), Cissp, SOX, Fisma, Compliance, Nist Certifications/Licenses CISSP GPEN GCFA Security+

Name: Scott Burns

Email: imurray@example.com

Phone: (484)357-2372