NERC CIP Cyber Security Specialist NERC CIP Cyber Security Specialist NERC FERC CIP Cyber Security Specialist Richmond, VA Authorized to work in the US for any employer Work Experience NERC CIP Cyber Security Specialist Burns and McDonnell-Contract Ending - Richmond, VA July 2017 to Present Support technical analysis of Industrial Control Systems (ICS) related to fossil and renewable Power Generation Systems for NERC CIP Compliance. For example ICS provided by Emerson, GE, Siemens, Vestas, etc. Maintain knowledge of the cyber security capabilities of operating systems, networking devices, control systems, and vendor offerings. Maintain a working knowledge of applicable cyber security standards involving electric power systems, including those relating to process networks. Inventory and asset management of cyber assets located at fossil and renewable Power Generation Systems. Develop, write, review, revise, and maintain security program standards and procedures for NERC CIP compliance. Understanding of security principles and good knowledge of cyber security technologies. General knowledge of control systems in use in the Electric Power sector, specifically those in Power Generation Systems. Operate in on-site industrial (Electric Power) work, and occasional night and weekend work. Demonstrated capability to make sound decisions based on good security practices and principles. Demonstrated understanding of business principles and operational security practices specific to engineering and/or security consulting. Experience with corporate policies and procedures and/or technical writing skills. Experience with physical cabling for network communications and control system I/O. Conduct research and work in collaboration with SMEs to validate policies, standards, plans, processes, and procedures to ensure compliance with regulatory requirements. Demonstrated understanding of IT process and infrastructure/ security related projects. Ability to read, analyze and interpret common engineering and technical network diagrams and communication protocols. Execute assignments for the Compliance & Critical Infrastructure Protection Group in the area of cyber security, Control/SCADA system configuration, preparation of documentation in support of data collection walk-downs at generation and transmission facilities, and contributing to the development of NERC CIP programs at client sites across U.S. IT Security Threat Analyst Entergy - The Woodlands, TX September 2015 to July 2017 Support the

deployment of security tools such as SIEM, IPS, physical security monitoring, etc. Leading and developing Smart Grid, SCADA, EMS, and DCS cyber security architecture and developing baselines, as well as monitoring, analyzing and producing reports and presentations based on data from multiple sources. Advanced support and leadership of complex applications and projects that require the integration of multiple security technologies (network, operating system, encryption, application, etc.) for Smart Grid, SCADA, EMS, and DCS environments. Advanced knowledge of security compliance policy, programs, processes, and metrics pertaining to NERC, FERC, NIST, and Smart Grid. Responsible for planning and designing processes for Smart Grid cyber security monitoring, incident detection, and incident response. Development, implementation, and on-going maintenance of security policies and procedures. Create business cases for investment in systems security (DLP, IPS, SIEM, etc) and include business value metrics in architecture, design, and implementation of security initiatives. Integrate security and data protection into business processes. Develop, publish, and utilize security and data protection standards and policies; enforce and audit adherence to published standards and policies. Identify new trends in systems security, data protection, and build business cases for adoption of best practices. Create, document, maintain, and publish / advocate vision and the business case for systems security and data protection. Define and document operational processes for running and supporting designed and implemented solutions (to ensure smooth hand-off to Security Operations and Administration team). Develop, implement, and operate controls to secure cloud-based systems. Utilize cloud-based APIs when appropriate to write network/system level tools for securing cloud environments. Recognize, adopt, utilize, and teach best practices in cloud security engineering. Participate in efforts to promote security throughout the enterprise and build good working relationships within the team and with others in the organization. Participate in efforts that tailor the company's security policies and standards for use in cloud environments. Develop reference architectures and proof of concept implementations of cloud security environments. IT Audit Manager CB&I-Chicago Bridge & Iron Company - Houston, TX November 2014 to September 2015 Coordinate staff requirements, scheduling and the assignment of work to be performed by others.

Review engagements and representation letters. Review the audit or other work programs and time budgets. Monitor each engagement to ensure that work is proceeding on schedule. Perform the most difficult phases of the work on larger and more complex IT assignments. Review and evaluate all work papers and determine compliance with professional standards and Firm policies. Make sure all documentation as required for Quality Control and Peer Review are included on all the assignments. Review reports, financial statements and tax returns. Review with the engagement partners any critical area or significant findings that raise questions involving accounting principles, auditing standards, tax regulations and Firm policies. Prepare and discuss staff performance evaluations on all staff under his/her supervision. Be involved in Practice Development type activities. Audit specific department for areas of process improvement and efficiency. Responsible for completing client work on timely basis. Responsible for billing to and collection from client. Delegate duties to subordinates and provide training. Develop and maintain good working relationships with client management. Follow and implement all aspects of The Sarbanes-Oxley Act, COBIT 5 and IT Governance. Determines the objectives and scope for each audit. Develops a Planning Memo to document the scope and objective. Conducts opening meeting with the business owner for the activity under review, and their staff, to discuss the scope and objectives of the audit. Flight Lead-Service Support Specialist II Universal Weather & Aviation, Inc - Houston, TX April 2013 to November 2014 Customer Station Supervisor / IT Support Spirit Airlines - Houston, TX August 2012 to April 2013 IT Support Manager- IT Medical Department/Facilities Ototronix, LLC - Houston, TX November 2010 to August 2012 Client Support Technician-ITO Trade Service Desk Hewlett Packard Company - Houston, TX January 2009 to March 2010 Customer Sales Information Specialist -Commercial Channel Operations June 2007 to January 2009 Client Credit Analyst II Enterprise Fleet Services - Houston, TX June 2006 to June 2007 Collections Manager / IT Customer Support December 2001 to June 2006 Call Back Center IT Support Representative December 2000 to December 2001 Education BA in Information Technology University of Phoenix - Houston, TX 2006 to 2010 Skills Cyber Security, Cissp, Information Security, Nist, Siem, Network Security, It Security, Information Assurance,

Cybersecurity, Linux, Comptia, IT (10+ years), Auditing (8 years), COBIT (8 years), Collections (7 years)

Name: Andrew Morgan

Email: melissawright@example.com

Phone: 001-382-427-6395x41480