

EXPERIENCE

SENIOR SYSTEM SECURITY ENGINEER

San Francisco, CA

09/2014 – present

- Help DoD customers develop strategic cybersecurity approaches for testing, and developing final solutions to secure Smart and microgrid initiatives
- Support customers' goals to create energy solutions that reduce energy use, reduce energy costs, and increase mission assurance
- Execute the DoD Risk Management Framework policies in accordance with DoDI 85001.01 Cybersecurity, DoDI 8510, RMF for DoD Information Technology (IT), CNSSI 1253, NIST SP, 800-53, SP 800-82 series publications, DHS ICS CERT publications and policies, along with local customer security directives to perform reviews of ICS system designs
- Perform best practice security testing for variety of ICS systems such as Utility Control Systems, (UCS) to include Supervisory Control and Data Acquisition (SCADA) systems, Advance Metering Infrastructure (AMI), Direct Digital Control, and various networked and non-networking Building Control Systems (BCS)
- Responsible for providing White papers, monthly technical reports, testing results and summaries, DoD RMF packages for respective DoD customer ATO approval processes, and executive summaries for technical and strategic initiatives to the customer's senior leadership
- Help address challenges to ensure DoD customers disparate legacy ICS are compliant with current DoD cybersecurity policy, and support the Project manager's management plan and provide inputs to update the plan when necessary
- 8 years working in the US NAVFAC, US Marine Corps, and or USACE ICS environment providing Cybersecurity testing plans, and security mitigations, and recommendations for ICS systems

INFORMATION SYSTEM SECURITY ENGINEER

New York, NY

07/2011 – 06/2014

- Applies knowledge of IA policy; procedures; and workforce structure to design; develop; and implement secure networking; computing; and enclave environments
- Assist the Government in developing and performing CSP staff training, training for users with elevated privileges, and general security awareness training
- Manage Secure System and Software Development Lifecycle programs
- Work closely with software engineers supporting and troubleshooting the deployment of our software on government-provided infrastructure
- Provides security planning; assessment; risk analysis; and risk management
- Manage accounts and network rights
- Assist in the development, implementation, and administration of effective security programs for approval by the Government

SYSTEM SECURITY ENGINEER

New York, NY

02/2005 – 01/2011

- 5) Develop advanced technological ideas and guide their development into a final product
- 3) Work on unusually complex technical problems and provide solutions which are highly innovative
- 9) Lead security business development and acquisition activities including proposal development, estimation and technical
- Manage of system security configuration
- 2) Work with subcontractors and commercial vendors in the selection and evaluation of secure operating systems,
- 1) Work on multiple simultaneous tasks
- Functional Analysis to create a Security Concept of Operations (SeCONOP) within the context of C&A

EDUCATION

HOWARD UNIVERSITY

Bachelor's Degree in Computer Science

SKILLS

- 2+ years experience in a high-availability 24x7x365 environment with highly structured change management
- Demonstrated solid understanding of general Linux systems administration
- Possess ability to implement policy, assign responsibilities, and prescribe procedures for applying integrated, layered protection of the systems and networks
- Strong technical understanding of system fundamentals and common Internet protocols
- Excellent English communication skills - written and oral
- Perform on-call duties as well as troubleshoot and fix open issues