Senior Cyber Security Reviewer Senior Cyber Security Reviewer Senior Cyber Security Reviewer - Securestrux LLC Atlanta, GA Work Experience Senior Cyber Security Reviewer Securestrux LLC 2015 to Present Serves as the Senior Security Readiness Reviewer throughout the world to provide expert consulting and auditing on vulnerability management and various network security configuration guidance for all Department of Defense networks. Provide and maintain situational awareness of Cyber Readiness Inspection results and mitigation status to include identification of key issues and priorities affecting the defense of the DOD Acquire threat and vulnerability data for inspected site and its geographical Area of Responsibility (AOR) to determine mitigation and remediation strategies Analyze and evaluate mitigation/remedial action plans of inspected sites using industry standard tools such as Tenable Nessus and Retina Identify systemic causes of inspection/assessment failures and develop recommended courses of corrective actions to increase defensive posture of the DODIN Provide analytical support to the CCRI process by reviewing CCRI results, operational reporting, and USCYBERCOM Threat Mitigation Framework (TMF) Analyze implementation plans and policies; analysis shall be specific to DOD but include familiarity with National Industrial Security Program (NISP) and National Institute of Standards and Technology (NIST) cybersecurity requirements and leverage industry and/or academia methods for addressing current and emerging cyberspace requirements Information Security Officer Federal Reserve Bank of Atlanta 2015 to 2015 Serves as the Bank's Information Security Officer and ensures the delivery of highly effective and efficient information technology (IT) and information security (IS) services to customers within the Sixth District. Plans, allocates resources, and directs the activities of the Information Security department in administering information security policy, procedures, and services for the Bank and in support of Federal Reserve System security initiatives. Leads the local incident response team (LIRT) and digital forensics by coordinating responses to information security events utilizing industry approved tools such as Volatility, and SANS SIFT distribution Coordinates with Federal Reserve System National IT on the delivery of national information technology and security services and the local deployment of Federal Reserve System technology initiatives. Helps develop and implement enterprise direction by actively

serving in leadership or individual contributor roles for national information security and information technology initiatives. Senior Malware Analysis Defense Contract Management Agency 2014 to 2015 Serve as the Senior Malware Analysis for the Defense Contract Management Agency Information Technology Division as the cyber expert in malware analysis by utilizing known static and dynamic malware techniques to uncover malicious code. Analyzed malicious code by conducting reverse engineering techniques and employing industry tools such ear Immunity Debugger and IDA Pro Manipulated reverse-engineering tools and scripting languages as well as virtual machine/networking software to undercover malicious code running on various machines Documented results in time-sensitive reports, presentations, and analyst exchanges for situational awareness and threat intelligence purposes. Identify and document high impact, emerging, and complex malware threats using proven industry methods. Collaborate with all peers within the Department of Defense Industry across the community to share finding and results with other departments. Supervised and mentored other Malware Analyst on the team. Information Assurance Officer National Defense University 2013 to 2014 Serve as the lead on National Defense University Information Technology Division as the cyber security specialist in by actively securing, monitoring, preventing, and detecting threats to National Defense University Faculty, Staff, and Students. Designed, architected, and built new vulnerability management system used to scan and detect known weak configuration and vulnerability published for remediation. Provided open source intelligence of unknown malware to partner agencies after discovering new malware variance. Changed the entire incident response and incident handling posture and procedure from a reactive posture to a proactive posture to better detect signs of compromise within a reasonable amount of time. Designed, architected, and built Universities System Incident Event Management system in order to better detect signs of compromise systems. Provide information assurance/information system security for networks that comprise a variety of data communication and computing devices (i.e., gateways, routers, terminal servers, modems, encryption devices and other INFOSEC products). Lead IT Cyber Security Specialist United States Marine Corps 2012 to 2013 Serve as one of the lead cyber security specialist in actively assisting the United States Marine

Corps in supporting their information security network and trusted system technologies. Designed, architecture, implemented, and managed entire Vulnerability management program (Retina & BigFix). Work collaboratively with security engineers, certification and accreditation, and external United States Marnie Corps institutions in order to improve the United States Marine Corps functions around the world. Security Analyst SMS Data Products Group, Inc 2011 to 2012 Served as a security analyst as a Computer Incident Response Team (CIRT) specialist in defending and protecting the United States Coast Guard network from bad actors and malicious content. Assisted in National Security missions set forth by the United States Coast Guard as a Computer Incident Response Team (CIRT) specialist with the assistance of the Department of Defense (DOD) Cyber Community in protecting and defending the United States Coast Guard Cyber Network. Monitor and actively mitigate cyber intrusions and anomalies using a variety of system security products exceeding Federal Department of Defense (DOD) and Department of Homeland Security (DHS) standards in securing various secure computer networks and systems. Conducted reverse engineering on various type of malware in order to gain and understanding and quick response of mitigation on potential malicious content. Education M.S. in Cyber Security Policy University of Maryland University College August 2013 B.S. in Mass Communications Frostburg State University December 2010 Certifications/Licenses CISSP Security+ GLSC GCIA GCFE CEH

Name: Sarah Brown

Email: nicolehopkins@example.org

Phone: 260-888-3782