IT Security Specialist IT Security Specialist IT Security Specialist - U.S. Department of Agriculture, ARS Washington, DC Work Experience IT Security Specialist U.S. Department of Agriculture, ARS - Beltsville, MD March 2017 to Present Pathways Cyber Security Trainee U.S. Department of Agriculture, ARS - Beltsville, MD June 2016 to March 2017 Combined overview of continuous duties: Key Accomplishments: Decreased the number of critical Adobe Flash Player vulnerabilities found on the network from 85% to 52% within two weeks. Created a custom fixlet on the BigFix console that remediated thousands of critical Adobe Flash Player vulnerabilities by upgrading all old versions. Reduced false positives on the network by deploying a fixlet that removed old registry entries of Adobe Flash Player from applicable systems. Deployed a baseline on the BigFix console that updated all applicable systems. Conducted extensive research and testing to create a more accurate way for the agency to track Adobe Flash player vulnerabilities. Communicated with the correlating vendor and agency POCs to officially validate the method as the best way to track the Adobe Flash Player installations. After implementing this new method, the Adobe Flash Player vulnerabilities within the environment instantly dropped from 938 to 51. Leadership is now looking into incorporating this new method within all USDA agencies. Made significant contributions in reducing the total number of high vulnerabilities on the agency's Cybersecurity Scorecard from 26 vulnerabilities per endpoint to 5 vulnerabilities per endpoint by assessing security events, identifying high/medium/low vulnerabilities and taking corrective action. Considerably helped remediate the WannaCry Cyberattack vulnerability by scanning systems and contacting correlating IT specialists to update their systems with the latest patch. Helped enforce the blocking of systems from the Network until they were successfully patched. These actions helped substantially protect the network from this notable ransomware vulnerability. Within four weeks of taking on management of the agency's Information Security Awareness training, I significantly increased the agencies score of completion from 49.1% to 85.3% through generating reports, analyzing data, sending out numerous emails, responding to inquiries through phone & email, contacting HR, contacting Area Directors, disabling accounts, collecting/storing certificates of completion and conducting investigative tasks. Previously, it took the agency 11 months to reach a

score of 49%. Received the highest-ranking score possible on recent performance appraisal. Routine Duties: Effectively and efficiently assesses system security events in the environment by utilizing multiple reliable security tools and tactics to identify risks and remediate vulnerabilities. Analyzes weekly CyberSecurity Scorecard reports, attends bi-weekly management meetings, generates BigFix Inventory/Web Security Reports, and conducts network scans through utilizing the Nessus (SecurityCenter) Vulnerability Scanner to identify, verify and evaluate vulnerabilities. Deploys security patches using the BigFix console, blocks MAC addresses and contact/assists correlating IT specialists in remediating critical vulnerabilities, such as WannaCry, Microsoft Office, Adobe Photoshop, Sever and RealPlayer vulnerabilities. Reduces the number of out-of-date and unsupported applications on the network through deploying the latest and greatest versions of critical software patches, as well as having any end-of-life applications removed. Ensures these actions do not negatively affect the environment by testing patches before deployment. Administers RSA Tokens and Personal Identity Verification ("PIV") card exemptions to maintain operations. Thoroughly assesses each exemption request and conducts investigations on personnel in question, to prevent and protect against unauthorized access to systems, network and data. Assisted in developing an RSA token disposal procedure. Reviewed and edited the agency's Penetration ("Pen") Test Remediation Process document. Reports, monitors and remediates Pen Test security assessment activities/findings. Utilizes previous penetration test results to find overlooked vulnerabilities. Led a BigFix Overview meeting on the implementation of the Vulnerability Management teams monthly restart strategy that would further secure the environment and drastically decrease the number of vulnerabilities on the network by allowing more systems to receive essential security patches. This strategy would also aid in immensely improving the Agency's Cybersecurity scorecard. Creates custom BigFix web reports and deploys custom vulnerability scans to aid customers in identifying vulnerabilities found on their systems. Knowledge of the step-by-step forensics process utilized within the environment. Provided multiple high- level recommendations to further improve the agency's Forensic policy. Attends weekly Vulnerability Management meetings to discuss new strategies to remediate critical and high

vulnerabilities. Involved in weekly Special Projects and Maintenance meetings to inform IT community on actions to take, actions to look out for, as well as to initiate discussions on any impending security subjects. Has presented information on efforts regarding unauthorized applications, PIV card exemptions and mandatory Security Awareness Training. Creates custom analyses within BigFix to verify vulnerability data found on thousands of systems. Resolves internal customer requests relating to tasks allocated to the CyberSecurity team through using BMC Remedy, a helpdesk platform. Personally, reaches out to customers and ensures that each request is handled in a timely and comprehensive manner. Creates agency communication documents that inform the Local IT community on important updates that could possibly cause changes in the environment. Sending out this form of communication has increased security awareness among the community, helped establish better communication and workflow, encouraged discussion, promoted awareness of security policies and procedures in a user-friendly manner, and reduced the number of possible negative mishaps that could occur while updating agency workstations and servers. Supervisor: Joe Kingston (301-504-5679); joe.kingston@ars.usda.gov IT Security Jr. Security Analyst Intern Washington, DC June 2015 to August 2015 Office of the Chief Technology Officer 200 I Street SE, Washington, DC 20003 (06/2015 - 08/2015) Hours per week: 25 IT Security Jr. Security Analyst Intern Performed continuous monitoring activities including the creation of VPN accounts and monitoring logs. Aided the Security Engineers and conducted research and submitted written reports on the D.C. government's VPN (Virtual Private Network) & SSL (Secure Socket Layer) process. Supervisor: Johnny West (202-478-9165); johnny.west@dc.gov Information System Security Branch Intern U.S. Department of Agriculture, FSIS - Fort McNair, DC June 2014 to August 2014 355 E Street SW, Fort McNair, DC 20024 (06/2014-08/2014) Hours per week: 25 Information System Security Branch Intern Utilized the Cyber Security Assessment and Management (CSAM) tool to monitor Plan of Actions and Milestones (POA&M) due dates and uploaded System Security Plans. 2 Reviewed/edited Security Policies, Standard Operating Procedures, and FSIS Taskers. Monitored the Office of the CIO's security dashboard for system reports and verified updates. Supervisor: Christopher Douglas (301-943-9894);

christopher.douglas@fsis.usda.gov Information System Security Branch Intern U.S. Department of Agriculture, FSIS - Fort McNair, DC June 2013 to August 2013 355 E Street SW, Fort McNair, DC 20024 (06/2013-08/2013) Hours per week: 25 Information System Security Branch Intern Monitored the Office of the Chief Information Officer's security dashboard for system reports and verified updates. Utilized Blue coat Proxy and Sourcefire to analyze intrusion events and user behavior. Supervisor: Christopher Douglas (301-943-9894); christopher.douglas@fsis.usda.gov Database Analyst Intern newBrandAnalytics Corporate Headquarters - Washington, DC June 2012 to August 2012 Performed data entry tasks including reviewing, editing and updating information on the social marketing database used by clients to improve the quality of customer service. Identified database errors to ensure links to the clients' websites were updated. Education Bachelor of Science in Information Systems in Cybersecurity University of Maryland - Baltimore, MD December 2016 Skills SECURITY (2 years), NESSUS (Less than 1 year), DATABASE (Less than 1 year), PHOTOSHOP (Less than 1 year), ADOBE PHOTOSHOP (Less than 1 year) Additional Information TECHNICAL SKILLS Programming: Java, Visual Basic Database: SQL Security: Nessus (SecurityCenter), BigFix, CSAM Media: Cisco 1 & 2 (CCENT I & II), Multi-Media Programming, Interactive Media I & II Adobe Illustrator, Adobe Photoshop, Computer Graphics

Name: Cheryl Colon

Email: ronnie93@example.com

Phone: (312)804-5200