Cyber Analyst IV - ARC Cyber Analyst IV - ARC Cyber Analyst IV - ARC - COLSA Corporation Huntsville, AL Mr. Hampel has 28 years of information technology experience with a total of 26 years of experience in information system security, 18 years of classified system security, cyber security and operational system support functions across multiple platforms. Authorized to work in the US for any employer Work Experience Cyber Analyst IV - ARC COLSA Corporation - Huntsville, AL June 2018 to Present Responsible for the effective installation/configuration, and maintenance of security hardware and software on systems of various Operating Systems. Additional duties include applying required system patches and mitigation of potential system vulnerabilities, system monitoring, verifying the integrity and availability of hardware, server resources, key system processes and the review of system/application logs. Provide guidance to lower-level employees. Required to have working knowledge and experience with reviewing and collecting action items from vulnerability reports. Responsible for working with the security teams, lab SAs and management in troubleshooting hardware/software issues and performing analysis on system problems. Responsible for implementing security system design specifications and defining input/output file specifications to include file organization. Responsible for defining controls, conversion procedures and system implementation plans. Responsible for managing and maintaining assigned classified systems. Principal Duties and Responsibilities (Essential Functions): Monitor the network and supporting systems to detect security compromise events (including intrusions and malware incidents). Provide weekly IAVM & Quarterly STIG notification and response auditing and tracking support. Run and audit Security Center (ACAS) scans and report archive process. Provide standard support for processes, investigations and maintenance of system accreditation Identifies where systems/networks deviate from acceptable configurations, enclave policy, or local policy. Provides recommendations for protecting networks, workstations, servers, and IT assets. Involved in conducting audits to ensure information systems security policies and procedures are implemented as defined in security plans and best practices. Supports the formal testing requirements through pre-test preparations, participation in the tests, analysis of the results, and preparation of required reports. Involved in passive evaluations (compliance audits) and/or active

evaluations (vulnerability assessments). Tracking/mitigation of potential system vulnerabilities Verifying the integrity and availability of hardware, server resources, and key system processes Review of system/application logs Provide guidance to System Administrators Use vulnerability reports to determine action items. Work with the security teams, lab SAs and management in troubleshooting hardware/software issues and performing analysis on system problems Analyzing security system design specifications, defining controls, conversion procedures and system implementation plans. Other duties as assigned Senior Information Technology SME Radiance Technologies Inc - Huntsville, AL February 2018 to June 2018 Provide subject matter expertise in the areas of Information Technology system configuration as well as Information Assurance (IA) support for Certification and Accreditation (C&A), Authorization and Accreditation (A&A), and DoD NIST 800-53 artifact production for RMF accreditation packages, policy generation, requirements analysis, security test plans, risk assessments, systems analysis, system hardening, incident response, Information presentations for company management and executive leaders, IA program assessments, and security posture presentations. Provide analytical support for the development and submission of C&A documentation in compliance with RMF framework requirements. Saved the company over 330K, within the first three months of employment, by accurately addressing Microsoft licensing options according to essential company software licensing requirements. Cyber Security Engineer, MDA ICVI Booz Allen Hamilton - Huntsville, AL January 2017 to February 2018 GML Provide subject matter expertise in the provision of Information Assurance (IA) support for Certification and Accreditation (C&A), Authorization and Accreditation (A&A), and DIACAP or RMF accreditation packages, artifact generation, requirements analysis, Security Test and Evaluation (ST&E) plans and execution, risk assessments, systems analysis and hardening, incident response and policy analysis, trusted product evaluations, IA program assessments, and security posture presentations. Provide analytical support for the development and submission of C&A documentation in compliance with the DIACAP or RMF framework. Apply knowledge of technology, analyze the security implications of systems and applications security, and provide recommendations to decision makers and engineers. Work with team members to provide advice

and assistance to facilitate C&A and A&A efforts. Traveled nationwide performing system security audit functions including ACAS scans on multiple classified systems. DoDIIS Security Manager USARMY Space Missile Defense Command G2 - Huntsville, AL 2008 to 2017 Huntsville, AL DoDIIS Site Security Manager, Information Assurance Manager, Information Assurance Security Officer, Information Assurance Network Officer, Sr. System/Network Administrator/Trusted Local Administrator, IT Specialist (2008-2017) Dedicated to perform a variety of technical and managerial tasks including establishment of DoDIIS program, policy and procedures for the effective implementation of selected cyber security controls, digital security requirements for JWICS operations. Action Officer for the production of Approval to Operate (ATO) system security authorization agreement (SSAA) documentation requirements for multiple Sensitive Compartmented Information Facilities (SCIFs). Including all aspects of Certification and Accreditation operational tasks; Configuration Management artifact documentation, Plan of Action and Milestones, Hardware Configuration List, Software Configuration List, Tempest Addendums, Appointment Orders for Information Assurance Security positions, and cost analyses for End of Life component replacements. Determine system technical specifications; implement software security configurations, system analysis for classified system integration determinations; and technical operational support. Develop, author and brief Insider Threat Mitigation Strategy for classified system users and system owners. Operate as a Trusted Local Administrator (TLA) for the administration of users data at the TS/SCI level; manage Public Key Infrastructure (PKI) implementation for encryption and digital signatures, assign system names and network addresses; monitor and evaluate network performance; install and configured hardware, update system images including Operating system software environments; evaluates hardware and software; trouble-shoot and resolved system and network functional and security relevant issues. Provide Cyber Risk Management support for both classified and unclassified systems, servers, networks and thin clients within an active directory structured environment. Work as a team member and independently to identify and recommend solutions that resolve complex system, server security and operational relevant issues. Author detailed plans for configuration changes and updates that apply directly to

JWICS, SIPR and NIPR systems. Provide technical support and training of SES level management and Military leaders regarding DoDIIS VTC and DVTC operations. As the Command DoDIIS Site Security Manager, Information Assurance Support Officer and Senior Systems and Network Administrator for TS/SCI systems, performed day to day operations in complete support for secure system operations within the JWICS environment. Responsible for enforcing security policies for workstation, server and network resources Assist with the mitigation of cyber relevant risks for network printing, system access and user rights Report and document Information System security violations Responsible for STIG compliance Research and assess new technology for functions pertaining to security and performance benefits Produce detailed plans and documentation for configuration changes and updates. Train Users regarding system security requirements for classified processing Considered a subject matter expert for information system security and cyber relevant issues Northrop Grumman Corporation - Huntsville, AL June 2000 to July 2008 System Administrator ISSO 2000 to 2008 Installation of classified and unclassified systems with hardened security configurations Hardware/Software technical support, audits and server administration Video and Image Editing for Class/Unclassified briefings Presentation Equipment Installation and Implementation Provide clear and effective solutions for the removal classified content from video images Prompt attention and correction of System/Server/User issues Backup and Restoration of classified data, configure user rights and profiles Research, Purchase and installation of various computer peripherals Passed Multiple DSS security audits for classified system processing IT Contractor Aero Tek - Huntsville, AL 1997 to 2000 Ghost drives and prepare systems for rollout Installation and configuration of new computer systems Performed complete Y2K system rollout Backup data, restored data, and restore email profiles Provided technical support, correcting all errors Live call technical support for professional level 3D graphic adapters Analyzed software and hardware installation procedure for compatibility Helped eliminate customer queue time by over 50% within one year Versatile communication and problem solving skills used daily Field Service Technician University of Alabama in Huntsville - Huntsville, AL 1992 to 1997 Provided service support for LAN/ WAN Scanned systems, removed malware, repaired damaged operating systems

Resourceful installation of software and hardware components for facility and staff computer systems, including consistent data transfers from Apple to PC systems Setup and configuration of computers, servers, printers, fax machines and display devices Proficient with solutions to fit fiscal budget requirements Design graphics for various university departments PC Technician, systems support MicroTechnologies - Huntsville, AL 1990 to 1992 Builder of customer specific 386/486 IBM clone computer systems Provided service and support for modem and RG-58 networking Installation of software and hardware components for customer computer systems, including virus detection and removal Setup and configuration of various video displays, printers, fax machines and pointing devices Education None University of Alabama in Huntsville - Huntsville, AL 1994 High school or equivalent Sparkman High School - Toney, AL 1989 Skills Cyber security, Firewall, Malware, Security, Active directory, Firewalls, Networking, System administration, Tcp/ip, Html, Scsi, Citrix, Remote access, Tcp, Vm, Red hat, Solaris, Linux, Sgi, Nist, Information Security, It Security, Information Assurance, Network Security, Cybersecurity Certifications/Licenses CEH December 2016 to December 2022 Certified Ethical Hacker ID# ECC14312861173 Certified Information Systems Security Professional (CISSP) August 2015 to August 2021 CISSP ID# 527590 DISA ACAS Version 5.3 (2016) Present enterprise Mission Assurance Support Service (eMASS) Present ASP - HP Client Virtualization -Remote Client Solutions Present DCID 6-3: Protecting SCI within Information Systems Present Information Assurance Security Officer (US ARMY IASO Mgt Level 1) Present Patents Securing stored computer files from modification (#10339328) https://pdfpiw.uspto.gov/.piw?Docid=10339328&homeurl=http%3A%2F%2Fpatft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO1%2526Sect2%3DHITOFF%2526d%3DPALL%2526p%3D1%2526u%3D%25252Fnetahtml%25252FPTO%25252Fsrchnum.htm%2526r%3D1%2526f%3DG%2526l%3D50%2526s1%3D10339328.PN.%2526OS%3DPN%2F10339328%2526RS%3DPN%2F10339328&PageNum=&Rtype=&SectionNum=&idkey=NONE&Input=View+first+page 2019-07 A computer system for securing computer files from modification may include a processor; at least a first data storage area operatively coupled to the processor; a non-volatile second data storage area; and a control circuit. The non-volatile second data storage area may be physically separate

from the at least a first data storage area. The second data storage area may store files that are executable by the processor, including executable files of an operating system configured to save temporary files on the at least a first data storage area. The control circuit may operatively couple the second data storage area to the processor, and may be operable in at least a first mode in which the control circuit is configured to block commands received from the processor and configured to modify the second data storage area from being communicated to the second data storage area. (Defeats Malware attempts to infect the protected data storage location(s)). Additional Information Inventor US Patent No.: US 10,399,328 Visionary innovator and co-inventor of the Secure Cyber Internal Lock (SCILock) Firewall Technology, designed specifically to protect computer system hard-drives, including the operating systems and associated programs within, from malware infection and future cyber security threats.

Name: Cassie Lopez

Email: shermanerin@example.com

Phone: 539.740.9356x21477