Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - AbleVets Laurel, MD Extensive background and experience in Information Security, IT infrastructures, and maintenance of large information systems. Experience using the appropriate tools to assess and analyze existing applications for system weaknesses and vulnerabilities and implementing techniques for mitigating security threats and risks. Experience with various compliance frameworks such as RMF, FISMA, NIST 800-37, NIST 800-53, FIPS, DOD SRG, FedRAMP, ISO, HITRUST, HIPPA, PCI-DDS and SSAE 16 (SOC 1 and SOC 2). Immensely knowledgeable of industry standards and proven track record of implementing the necessary controls to ensure compliance. Work Experience Cyber Security Analyst AbleVets - Chantilly, VA July 2018 to Present * Identify security risks through the analysis of known information. * Assess the Cyber Security risk of IT systems documenting them in formal risk assessments and supporting artifacts associated with the A&A process * Organize, develop, and present security briefings, written summaries, and written reports incorporating narrative, tabular, and/or graphic elements on A&A activities * Implement IT security solutions and assure successful implementation * Apply knowledge of security principles, policy, and regulations to daily tasking * Provide IT security analysis support to cross-functional project teams to ensure that VA security policies, processes, and controls are adhered to, planned for, implemented throughout the project lifecycle, and provide strategic cyber security support for OIS * Support projects from initiation and throughout the development lifecycle to provide hands-on security subject matter expertise and support to include assisting in knowledge transfer, VA Agency specific security policy and controls coaching, and drafting of security documentation * Research policies, procedures, standards, and guidance, and applies needed changes under specific conditions for the protection of information and information system Information Assurance Analyst Prometic Biotherapeutics - Rockville, MD February 2018 to July 2018 * Proactively identify weaknesses and their root causes to mature the IT controls environment. * Drive comprehensive recommendations for remediating complete problems identified from external and internal audits. * Coordinate and monitor remediation activities across the department. * Provide support for management of groups that comprise of CIO, CISO, CFO, and various division representatives. * Work closely with

management and leadership to provide briefings on status of weaknesses and security environment.

* Develop standardized methodologies for validation of remediation actions for identified weaknesses to ensure effectiveness at the design and operation level leveraging HIPPA, SOC 2, NIST 800 - 53 frameworks. * Identify entity wide IT control issues that are pervasive among multiple systems and provide recommendations for plan of actions. IT Security Assessor Georgetown University Medical Center - Washington, DC December 2015 to January 2018 Managed the information security function in accordance with the established policies and guidelines. Established and maintained information security policies, procedures, and guidelines pursuant to state and federal laws and regulations such as the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) memorandums, and Department of Homeland Security (DHS) binding operational directives. Assessed security and privacy controls using the NIST SP 800-53A, PCI DDS and HIPPA publication guidelines. Reviewed security policy documents and made recommendations on documentation compliance. Conducted and performed continuous monitoring pursuant to NIST guideline requirements. Provided impact analysis for updates and version changes required by the NIST security publications and FISMA notices. Responsible for tasks related to the system Assessment and Authorization (A&A) and follow the government IT security policies and standards. Conducted meetings with the client to discuss client's material weaknesses identified in an audit to gain an understanding and develop mitigation strategies for the findings. Met with system point of contacts to discuss and provide guidance on remediation strategies. Communicated complex technology and security concepts and methodologies to senior leadership to support development of enterprise security strategy implementation. Served as a subject matter expert in governance and leadership by reviewing and developing effective structure for communicating, decision making and responding to security threats across an organization. Consultant Deloitte - Washington, DC April 2012 to December 2015 Provided expertise on technical services including all aspects of information security. Conducted IT risk assessments to identify system threats. Assessed system design and security posture as well as advising information security compliance with FISMA and NIST SP 800-53 controls.

Performed maintenance and advanced configuration of systems to protect systems from emerging cyber threats. Conducted reviews of processes, policies, procedures, security, and configuration controls of existing systems as well as proposed controls for new systems. Provided mitigation strategies and recommendations to key stake holders to enhance their security posture. Education Masters of Science in Cyber Security Management and Policy University of Maryland University College - Adelphi, MD May 2019 Masters of Science in Physiology California State University - Hayward, CA Bachelors of Science in Biology California State University - Hayward, CA

Name: Aaron Simmons

Email: lewisglen@example.com

Phone: 9005131226