Guardsight, Inc. | 755 S. Main St., #4-137, Cedar City, UT 84720 | 844-482-7374

Senate Bill 235, An Act Establishing a Cybersecurity Task Force
Public Safety and Security Committee
March 5, 2020

My name is John P. McGloughlin, Founder and CEO of GuardSight, Inc. of Cedar City, Utah. I am a Certified Information Systems Security Professional (CISSP), co-author of a Cyber Security Analytics Architecture patent, a member of the Industry Advisory Board for Southern Utah University, an Occupational Advisory Committee member of Southwest Technical College, a Marine Corps Cyber Auxiliary civilian volunteer, an InfraGard member, and an Infrastructure Liaison Officer.

Established in 2009, GuardSight provides specialized cybersecurity services to various industries, including retail, entertainment, banking, finance, insurance, education, technology, real estate, biopharma, manufacturing, sports, Internet, and data science. Our cybersecurity protection packages complement our elite and reliable cybersecurity experts. Our managed threat detection and response services, help small businesses and large enterprises, including governmental entities, effectively manage their cybersecurity. GuardSight has extensive experience in many areas of technology and information security, including network engineering, software development, systems administration, vulnerability management, cyber intelligence management, cybersecurity operations (SECOPS), and incident response.

Senate Bill 235 establishes a cybersecurity task force that is charged with developing a strategic plan and submitting a report on its findings and recommendations concerning several items. The responsibility of the task force will entail collaboration with the private sector to facilitate cybersecurity, including efforts related to corporate espionage, protection of trade secrets, and data privacy. **GuardSight enthusiastically supports Senate Bill 235 and urges the Public Safety Committee to approve the bill**. I want to thank the committee for introducing the bill and Sen. Tony Hwang for his leadership on cybersecurity issues.

Connecticut has been a leader among the states in cybersecurity strategy, action plans, and awareness. It has shown tremendous foresight and serves as a model for other states to follow. The state recognizes the immeasurable safety and competitive advantage gained by adopting these policies. By establishing a cybersecurity task force, the state can continue its leading role in public policy concerning the importance of cybersecurity.

By way of background, in 2014, Governor Malloy adopted a cybersecurity strategy to cover vital public utilities and launched an action plan. In 2017, the state adopted an official Connecticut Cybersecurity Strategy developed by Chief Information Officer Mark Raymond and then-Chief Cybersecurity Risk Officer Arthur House. The strategy aimed at developing a unified understanding of the nature, ubiquity, urgency, and persistence of the cyber threat and putting

the entire state on the same path. Its primary audience is Connecticut's leaders, including in the General Assembly.

The strategy helped form a pathway to a more detailed, operational action plan, which was adopted the following year. Connecticut's Cybersecurity Action Plan sets forth specific steps necessary to strengthen the state's ability to defend against and recover from cyber compromise. It affects coordination between government entities with a focus on state and municipal government, the private sector, institutions of higher learning, and law enforcement. Together, Connecticut's Cybersecurity Strategy and Action Plan are a "call to arms to prepare for, prevent, respond to and recover from threats to cybersecurity infrastructure at the state, local and private-sector levels."

Additionally, the state has developed a website designed to provide resources for all levels of Connecticut users, from home computing to businesses and government organizations. It provides links to recommendations and best and safe practices from a variety of sources that can improve understanding of the cyber environment and how to use that environment more securely. It provides resources for small businesses and comprehensive guidelines to prevent computer risks.

The task force does not have to reinvent the wheel. In fact, Connecticut's Cybersecurity Strategy and Action Plan, already in place and being implemented, could complement and help inform the task force and shape its deliberations and work product. One of the challenges GuardSight has experienced is workforce development and finding qualified cybersecurity workers. Data shows that cybersecurity talent gaps exist across the U.S., including in Connecticut. The task force should support the efforts of state officials by continuing to review the workforce needs to identify what should happen to build the next generation of workers skilled in cybersecurity defenses. By collaborating with the private sector, the task force can help identify and address these challenges.

The Cybersecurity Strategy emphasizes workforce development. It recommended that the General Assembly cultivate cybersecurity cultures to underscore that cybersecurity is not merely an information technology problem. "To ensure that it is part of every agency mission and job description, Human Resources must tailor recruitment to a workforce that lacks adequate cybersecurity skills, by seeking new hires with the talent and attitude to commit to cyber awareness amid resource scarcity."

GuardSight commends the committee, policymakers, and the Connecticut General Assembly for their foresight and leadership in cybersecurity. I would be happy to serve as a resource to the cybersecurity task force as it begins its work to address the challenges ahead.

Please contact John McGloughlin, (844) 482-7374 or john.mcgloughlin@guardsight.com, with any questions or for additional information.