



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

House Bill 6607, An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses

Commerce Committee

March 18, 2021

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 Cybersecurity Analytics Architecture patent, a member of the Industry Advisory Board for Southern Utah University, an Occupational Advisory Committee member of Southwest Technical College, a Secure The Village Cybersecurity leadership council volunteer, a National Child Protection Task Force volunteer and Cybersecurity Advisor, a Utah volunteer firefighter/first responder, 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 many types of organizations – from small businesses to 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.

GuardSight supports House Bill 6607 and urges the committee to approve the bill.

The bill is a reasonable public policy measure that would encourage companies to adopt Cybersecurity standards that will protect businesses and consumer data and information and help make both less vulnerable to attack. Additionally, HB 6607 supports small businesses and makes Connecticut more attractive to resident companies and others seeking to relocate to the state.

House Bill 6607 provides an affirmative defense to businesses that adopt a prescribed Cybersecurity program to protect personal information and are subject to a tort claiming



an alleged failure to implement reasonable Cybersecurity controls that resulted in a data breach.

The standards in HB 6607 provide a positive way of protecting consumer information rather than imposing fines on businesses. In 2018, the American Bar Association supported a similar measure in Ohio, saying it provides “a unique incentive for voluntary compliance with cybersecurity measures that contrasts to laws in other states, like New York and Massachusetts, that punish noncompliance with cybersecurity provisions.” The bill does not provide immunity from such claims. Consumers could claim other statutory violations or rely on contract theories for a cause of action. Additionally, eligibility for the affirmative defense presents significant challenges. A business must show that it “created, maintained and complied with a written cybersecurity program” and it must comply with designated industry or government Cybersecurity frameworks.

When it comes to Cybersecurity breaches and insurance, some companies have found themselves losing on multiple fronts, including significant property damages, devastating business disruption, extortion, career destruction, and later discovering the insurance claim is declined. Some insurers have even denied coverage for breaches citing “Act of War” exclusion clauses. Cyber standards can help resolve this challenge by reducing risks for companies. Standards will not only assure a standard of due care, but they will also protect consumers and proprietary information.

Cybercriminals continue to advance their levels of sophistication. They are increasingly finding ways to breach computer systems and steal consumer data. State policies should encourage companies to adopt industry-recognized Cybersecurity frameworks such as NIST’s special publications and the ISO/IEC information security standards.

House Bill 6607 is a business-friendly measure that makes Connecticut more attractive to companies, which will, in turn, help create and grow jobs in the state. Contrary to conventional wisdom, cyber attacks do not mostly impact large, high-profile companies and organizations. In reality, small to medium-sized businesses (SMBs) are the most vulnerable and frequently represent an attractive “soft target” opportunity for cybercriminals. The SMB victim of a significant Cyber attack often experiences extreme monetary ruin and is oftentimes shuttered completely. In some instances, the SMB supplies a conduit for access by the Cybercriminal into the large “hard target” businesses through the supply chain, resulting in everything from large-scale theft to espionage to danger to citizens themselves. HB 6607 encourages improvements to cyber hygiene and posture using practical and reliable standards, making companies of all sizes less vulnerable to attack, thereby protecting assets, critical infrastructure, intellectual property, consumer data, and national secrets.

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 considering and adopting these policies. Indeed, just yesterday, Governor Lamont announced the launch of a year-long process for building a new information technology organization within state government that will include improving Cybersecurity. The administration indicates dealing with potential threats would be improved by having a centralized team and consolidated systems for the state workforce. When everyone is working on fewer, more secure, and updated platforms, risks are lowered. Most Cybersecurity companies and experts would agree with those best practices. By incentivizing the adoption of Cybersecurity standards, the state can continue its leading role in public policy concerning the importance of Cybersecurity.

GuardSight commends the committee, policymakers, the Connecticut General Assembly and the Governor for your foresight and leadership in Cybersecurity. Our company stands ready to serve as a resource to state officials as you consider and develop Cybersecurity standards and policies.

For questions or additional information, please contact:

John McGloughlin | CEO
w: <https://www.guardsight.com>
e: john.mcgloughlin@guardsight.com
o: 844-482-7374
k: 0x04646E35BE3049B2