MASSACHUSETTS
HIGHTECHNOLOGYCOUNCIL
Dedicated to Growth... Committed to Action

TESTIMONY

Submitted to the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity

Written Testimony Related to the Committee's July 13, 2023, Committee Hearing

Elizabeth Mahoney, Vice President of Policy and Government Affairs
Massachusetts High Technology Council

Dear Chair Moore, Chair Farley-Bouvier, and Members of the Committee,

Thank you for the opportunity to submit testimony. My name is Elizabeth Mahoney and I'm the Vice President of Policy and Government Affairs for the Massachusetts High Technology Council, the Commonwealth's oldest cross-sector association of CEO-level leaders of technology, professional services, and research institutions. The Council has a 46-year history of non-partisan advocacy in support of our mission to make Massachusetts the world's most attractive place in which to live and work, and in which to create, operate, and grow high technology businesses.

Last year, the High Tech Council launched MassVision2050, a multi-year initiative that brings together private, public, and academic leaders to generate bold ideas for Massachusetts' future, focusing on the most important trends in technology and their implications for Massachusetts, with an eye towards supporting the key sectors that are likely to drive employment and economic growth in Massachusetts in the coming decades.

Focusing on nine sectors, including Artificial Intelligence and Cybersecurity, our goal is for MassVision2050 to help guide and shape policy decisions by providing bold, fact-based recommendations for public, private, and academic leaders.

Some initial facts we've compiled on AI and Cybersecurity:

- Massachusetts' supply of AI talent ranks fourth in the country, as does our number of new AI-related jobs since 2019.
- An estimated 14,000 Massachusetts-based workers have AI-related roles or skills, and our state's employers are more likely to be looking for AI talent than the rest of the country is.
- Massachusetts ranks 10th amongst US states for new cyber-related jobs, and we are one of just two states among the top 10 that are close to producing enough graduates to meet the industry demand.

As this Committee considers how to provide robust consumer protections and appropriate guardrails around new and emerging technologies, the High Tech Council would like to offer its thoughts on how to do so while also supporting the growth and innovation of these industries.

Ensuring artificial intelligence is used in a way that's safe, fair, and accurate will be critical when incorporating AI into the work of various industries, including state government.

H64 and S33, which would establish a commission on automated decision-making by government, would be a good way to explore the benefits and risks of incorporating the use of AI into state government and the High Tech Council would be pleased to serve on such a commission. We would suggest the commission consider how to leverage the work of other states and federal government entities working on these issues, while also addressing the specific needs of Massachusetts.

S.31, drafted with the help of ChatGPT, would regulate generative AI models like ChatGPT. Establishing sensible guardrails around such technologies is a good idea, although there are a couple of aspects of this bill that could use further clarification. For example, how the requirement to "obtain informed consent from individuals before collecting, using or disclosing their data" would apply to data that is already publicly available. Also, it is worth considering the rapidly evolving nature of this technology, and what is defined in this bill as a "large-scale model" will likely not be a large model in the near future – there should be an opportunity to update that definition over time as the technology evolves.

On cybersecurity, there are several bills before you that would better prepare the Commonwealth to prevent and respond to cyber incidents and update existing state laws around the protection of personal data.

S.36 would establish a cybersecurity control and review commission, and require companies working with the Commonwealth to meet certain cybersecurity standards. To avoid complications for businesses seeking to meet these standards, it is advisable that the commission focus on identifying U.S. standards that already exist and adopting those, rather than creating a new set of standards, and we appreciate that the bill requires the commission to base the standards on the National Institute of Standards and Technology Cybersecurity Framework. One recommendation is that the Commission work to understand the challenges small businesses face in meeting cyber standards so that smaller businesses are not inadvertently shut out from working with the Commonwealth.

H.76 and S.30 would revise the existing data breach notification law and we support this effort to clarify and update the sensitive information that must be protected. We do believe there could be further improvements made to the notification process for those impacted by data breaches which would better enable them to avoid fraud. For example, the notifications that impacted consumers receive are static and only represent what the company knows about a data breach at the time the notifications are sent. But companies frequently learn more about the extent of a security incident over time, including whether and how compromised customer information may have been misused. Relatedly, the notifications that companies send to their impacted customers may not adequately explain what criminals could do with the customer's information and why it is important for the customer to take steps to protect themselves. Consumers impacted by data breaches would be well-served if companies sent them not just an initial notification but also notification updates several months later, as well as more clearly explaining in those notifications what risks the consumer may have been exposed to.

S.32 would establish centralized oversight, reporting, and preparation for cyber incidents within the Commonwealth, which is a good idea and should include using a risk management approach to assess the vulnerabilities of critical infrastructure and primary impact areas. We recommend engaging the private sector in the work of the Cyber Incident Response Team as many cyber incidents impact both the public and private sectors and can be better contained with public/private cooperation. An organization like the Advanced Cyber Security Center—a New

England-based alliance of cyber executives, risk officers, and legal counsels—may also be worth consulting for their expertise. There are also good models in other states that could be helpful to inform the work of the Response Team; state programs worth reviewing include Arizona, New Jersey, and Washington.

While there are many challenges to consider with these new technologies, there is also an opportunity for Massachusetts to be a global leader in the innovation and development of these sectors. The High Tech Council would welcome the opportunity to continue to engage with this committee on these topics and to share the insights and recommendations that are generated through our MassVision2050 initiative.

Thank you for your consideration.