



November 12, 2025

The Honorable Thaddeus Claggett, Chairman
Ohio House Technology and Innovation Committee
1 Capitol Square
Columbus, Ohio 43215

Dear Chair Claggett, Vice Chair Workman, Ranking Member Mohamed, and members of the House Technology and Innovation Committee,

We would like to submit feedback on HB 392 as an interested party. We believe it is important to provide insight and perspective on regulation that may impact public safety and critical infrastructure.

Our feedback is in two key areas: ensuring that risk management regulations effectively apply to all critical infrastructure deployments and that state and local government technology standards can remain effective.

Cybersecurity and safety concerns for critical infrastructure

Risk management practices for artificial intelligence deployed in critical infrastructure need to be introduced at the onset of a project, not after deployment.

Issue: The legislation states that “(C)(1) Any person or other entity that implements or operates an artificial intelligence system that in whole or in part controls a critical infrastructure facility shall, before *or within a reasonable period after the deployment of the system*, implement a risk management policy.” Risk management is a holistic process that includes generation of system requirements for safe, secure, and reliable systems before deployment. “Bolting on” risk management practices afterwards opens opportunities for unmitigated risk and often forces the deployment of expensive or substandard secondary controls after the system has already gone live. One of the biggest challenges of critical infrastructure is that maintenance and upgrade windows for improvements introduces the risk of outages and increased costs.

Voluntary risk management frameworks do not take into account that some systems are inherently more high risk and consequential than others. Those categories have to be predetermined so that the expectations for their deployment are complied with before they are operational.

Proposed Remedy: Strike the “*or within a reasonable period after*” language in the legislation.

All artificial intelligence projects that impact the integrity and availability of critical infrastructure must introduce risk management practices without exception.

Issue: The legislation states that the risk management requirement for critical infrastructure does not apply “if the artificial intelligence system is exclusively an antivirus, antimalware, or cybersecurity tool.” Carveouts for cybersecurity tooling are inappropriate, as such tooling may deny access to operators in case of an emergency. If the system does not require risk management review and implementation due to the exception, there are critical gaps in safety and security. One only has to look at the 2024 CrowdStrike outage that crippled industry, transportation, communications, and other critical infrastructure functions to see how risk management failures resulted in significant impact caused by security tooling. It is recommended that additional language around risk management frameworks mandate the presence of a “kill switch” that would allow manual override and operation by human operators.

Proposed Remedy: Strike the “or if the artificial intelligence system is exclusively an antivirus, antimalware, or cybersecurity tool” language in the legislation.



Restrictions on agencies and other political subdivisions threatens creation of meaningful security and privacy policy and guidance to protect Ohio citizens

Policies and practices that impact state and local deployments of technology should be considered part of the compelling government interest exception.

Issue: As an example, the Ohio Department of Administrative Services has published a policy on the use of artificial intelligence for state agencies, boards, and commissions under the authority of the Governor. If the definition of “any person” is interpreted as to include the IT or operations staff of an Ohio state agency, then these standards would no longer be in effect. These standards have ensured the protection of personally identifiable information of Ohio citizens and confidential state information when adopting generative AI solutions.

Outside of artificial intelligence standards, there are essential security and privacy requirements maintained by state agencies and political subdivisions by their very nature restricts or prohibits the use of computational resources by state employees in the course of their employment or by departments executing the normal course of business. These policies prevent unauthorized use of technology or misuse of resources that would not necessarily rise to the standard of unlawful conduct, but would still put confidentiality of citizen data and availability of government services at risk.

Proposed Remedy: Add “technology standards issued by state agencies and political subdivisions for the purposes of risk management within those state agencies and political subdivisions” explicitly to the list of compelling governmental interests in (1). Alternatively, establish an exclusion to the “any person” definition for government use and adoption of technology.

Policies and practices that impact business or individual usage of state agency or political subdivision computational resources should be considered part of the compelling government interest exception.

Issue: State agencies and political subdivisions provide many online services to their constituents and in some cases, act as Internet service providers. Acceptable use policies, rate limits, and technical controls are necessary to prevent abuse of these services and to ensure availability for all citizens, and not all cases of misuse would be considered unlawful or fraudulent. The legislation as written prohibits these entities from creating reasonable controls to protect their services.

Proposed Remedy: Provide sufficient latitude for agencies and political subdivisions to control usage of their services offered to businesses or individuals within the state.

We appreciate the opportunity to provide feedback on this legislation and are available to answer any questions the committee or sponsors may have moving forward.

Mehtab Khan

Assistant Professor of Law at Cleveland State University College of Law

Cory Scott

Executive Director, Center for Cybersecurity and Privacy Protection at Cleveland State University



Mehtab Khan Biography

Mehtab Khan is an Assistant Professor of Law at Cleveland State University College of Law, where she teaches Intellectual Property, AI Law, and other tech-related subjects. Professor Khan is an expert on copyright law, platform governance, and artificial intelligence. Her recent academic scholarship includes articles on developing an accountability framework for large-scale AI training datasets, regulating automated content moderation and online speech tools, and the impact of AI on the creative industries.

Professor Khan was previously a Fellow at the Berkman Klein Center (BKC) at Harvard University. Her research at BKC examined ways of governing the practices involved in developing and deploying AI technologies. She is particularly interested in ensuring diversity and representation in the development process. She has also held positions at Yale Law School, serving as a Resident Fellow at the Information Society Project and as the Program Director for the Yale/Wikimedia Initiative on Intermediaries and Information. Additionally, she has been a visiting researcher at Stanford HAI. She is a recipient of numerous grants to work on the use of AI in hiring. In 2019, she was a Fellow at the Center for Technology, Society and Policy and a Research Grantee at the Center for Long-Term Cybersecurity.

Her doctoral dissertation, completed at Berkeley Law, examines the role of internet platforms in shaping fair use. This research was partly inspired by the challenges internet users face in accessing knowledge and the ways platforms like Google and Wikipedia navigate complex copyright rules to make knowledge more accessible.

Professor Khan is a licensed attorney and has previously worked as a lawyer in the United States, Malaysia, and Pakistan. She has held positions at the Wikimedia Foundation, Creative Commons, and the Electronic Frontier Foundation—three Bay Area institutions that have been at the forefront of many legal battles around digital rights. She holds an LLM and JSD from the University of California, Berkeley School of Law.

Cory Scott Biography

Cory Scott brings over 25 years of cybersecurity expertise spanning both private industry and public service. His career has included vulnerability research, forensics, and incident response at leading consultancies, as well as security leadership roles at major financial institutions and technology companies including LinkedIn, Microsoft, Google, and Confluent.

Currently, he is dedicating his time to public service and security research. He serves as Deputy Regional Lead for the Cleveland branch of the Ohio Cyber Reserve, part of the Ohio Military Reserve focused on protecting state governmental bodies against cyber attacks. He also sits on the advisory board of CyberOhio, where he helps advise the governor on public policy initiatives involving collective defense and critical infrastructure protection.

As the newly appointed Executive Director of Cleveland State University's Center for Cybersecurity and Privacy Protection, he focuses his research on three key areas: cybersecurity for public sector organizations and critical infrastructure, including policy analysis of how collective defense strategies impact citizens and communities; data protection strategies for large multi-tenant service providers; and the evolving practice of cybersecurity—particularly its intersection with legal practice and professional ethics.

Scott has presented his research and insights at major industry conferences including Black Hat Briefings, USENIX, OWASP, RSA Conference, and SANS.