POLICY MEMORANDUM

Establishing a State-Level Strategy for Managing Systemic Cyber Risk in Massachusetts

TO: The Office of the Governor of Massachusetts

FROM: Lauren Zabierek, CEO & Co-Founder, Software Safety Institute | Senior Advisor, CAS Strategies | President, LZX Consulting | Former CISA Senior Advisor

DATE: June, 2026

PURPOSE

The Commonwealth of Massachusetts currently lacks a coherent strategy or designated institutional owner for managing systemic cyber risk to critical infrastructure. This memorandum highlights this gap in the Commonwealth's approach to cybersecurity and recommends a targeted set of actions to address it.

BACKGROUND

Massachusetts has made meaningful progress on technology innovation, including through the MassTech AI Hub and SHIELD initiative, and maintains baseline cybersecurity programs across state agencies and municipalities through the work of EOTSS, EOPSS, and the MassCyber Center. These are real achievements. However, recent adversary activity illustrates a class of threat that existing state structures are not designed to address, and which will only intensify with AI tools.

The Littleton Case

Just up the road from Boston's technology corridor sits Littleton Electric Light and Water Department, a small, under-resourced water and electric utility that became a target of Volt Typhoon, a state-sponsored cyber campaign attributed to the People's Republic of China. Discovered in 2023, the intrusion involved actors compromising the utility's network and "living off the land," passively observing and pre-positioning to disrupt water and energy operations should the United States intervene militarily in a conflict over Taiwan. Littleton is now bearing the substantial costs of remediation, response, and recovery. That a community like Littleton sits within miles of a multi-billion dollar technology ecosystem, yet faces this threat largely alone, illustrates the structural gap this memo addresses.

Littleton is one of hundreds of known Volt Typhoon compromises across the United States and Guam. What makes this campaign particularly damning is how initial intrusions were achieved: through exploitation of well-known, preventable vulnerabilities and misconfigurations in edge network devices such as firewalls and routers—the very tools intended to protect these networks. This insecure software is permitted on the market because there is insufficient legal liability for the harm it causes and little incentive for manufacturers to build it securely.

Reductions in federal cybersecurity capacity over the past year have compounded this challenge. CISA's regional cybersecurity advisors departed the agency in significant numbers, leaving gaps that the Commonwealth has no current mechanism to fill. Executive Order 14239 ("Achieving Efficiency Through State and Local Preparedness," March 2025) formalized this transfer of burden, shifting substantial responsibility to state, local, tribal, and territorial governments without commensurate funding, staffing, or capacity building.

> ***States have to step up in the vacuum of federal action. Massachusetts has the standing to lead in this space, and the potential to build regional coordination***

> ***across New England. What it currently lacks is the structure, the mandate, and the dedicated resources to do so.***

CHALLENGES

CHALLENGE I — NO INSTITUTIONAL OWNER OF SYSTEMIC CYBER RISK

States and municipalities are increasingly expected to manage cyber risk to critical infrastructure, despite that risk being created upstream through insecure software design decisions made by manufacturers operating without liability or meaningful market pressure. Massachusetts does not currently have a defined owner of systemic cyber risk, a policy framework that treats cyber as a public safety issue, or a mechanism for integrating cybersecurity considerations into cross-sector operational and procurement decisions.

The current approach to managing risk remains largely reactive: tabletop exercises, incident response planning, and phishing awareness training. Organizations such as MassCyber and initiatives like CyberTrust Massachusetts represent genuine achievements. But they operate downstream of the problem. The most effective intervention in preventing compromise is not better response; rather, it is secure software with secure defaults. This is not a technological impossibility; it is a question of incentives and policy, one that the federal government is not currently postured to address.

CHALLENGE II — EXISTING STATE STRUCTURES ARE REACTIVE AND BOUNDED IN SCOPE

An acute issue is that no existing body is positioned above these agencies, able to synthesize their visibility into a statewide picture and act on it from a policy standpoint. Current capabilities are meaningful but not designed for persistent, systemic threats:

- **MEMA and ESF-17** provide incident coordination in crises, not upstream risk reduction. Current resourcing may be insufficient for a Volt Typhoon-style scenario involving simultaneous electric and water disruptions affecting hospitals when CISA has been degraded.
- **MassCyber Center** municipal support programs focus on local capacity building. They are not structured to provide statewide exposure analysis, advise the Governor’s office on systemic risk, or inform legislative priorities.
- **The Executive Office of Public Safety and Security (EOPSS)** oversees the agencies most directly responsible for emergency response, law enforcement, and physical infrastructure protection including MEMA and the Massachusetts State Police Fusion Center, and does have relevant cybersecurity activity: an internal CISO managing information security across its 12 secretariat agencies, and an Office of Grants and Research that serves as the State Administrative Agency for federal DHS/FEMA cybersecurity grant funds. The 2020–2023 Homeland Security Strategy states cyberattack prevention and response as Goal 4. But none of this constitutes a mandate to assess systemic risk across sectors, advise the Governor on critical infrastructure exposure, to treat insecure software design as a public safety policy issue, or take ownership of the cross-sector, upstream risk problem this memo addresses. That gap is what must be filled.
- **The Executive Office of Technology Services and Security (EOTSS)** is the Commonwealth's lead enterprise technology organization, and it does meaningful cybersecurity work: it sets enterprise information security policy for over 125 executive branch agencies, operates the Commonwealth Security Operations Center, runs the MA Cyber Incident Response Team (MA-CIRT) jointly with EOPSS, administers cybersecurity awareness training across state government, and chairs the IT Investment Advisory Board. These are real capabilities. But EOTSS's mandate is fundamentally inward-facing, securing the Commonwealth's own IT environment and workforce. It does not have authority or structural position to assess cyber risk to privately operated critical infrastructure such as

water utilities, hospitals, or energy systems; to advise on software manufacturer accountability; or to set procurement security standards that flow to municipalities. The IT Terms and Conditions it jointly administers govern executive branch purchases but, as noted below, have not been updated to require Secure by Design baselines. EOTSS is a capable technology governance body operating within a defined lane, but the systemic risk problem sits outside that lane.

- **Home Rule deference** means municipalities are not required to adopt security standards, producing uneven baseline protections and limiting the state's ability to assess aggregate exposure.
- **Sector regulators such as MassDEP** are beginning to integrate cybersecurity into facility-level oversight but lack authority, resources, and data to address system-level risk.
- **The Department of Public Utilities (DPU)** regulates electric and gas utilities but exercises limited cybersecurity oversight. The Commonwealth has no mechanism to assess aggregate exposure across its energy systems.
- **The Department of Public Health (DPH)** licenses healthcare facilities but has no cybersecurity mandate. Hospitals are high-value ransomware targets whose compromise intersects directly with the MEMA scenario above.

CHALLENGE III — AVAILABLE POLICY LEVERS DO NOT ADDRESS ROOT CAUSES

Massachusetts has real tools at its disposal: MassCyberCenter training programs, EOTSS security policies, sector-specific compliance requirements, and incident response frameworks. These are not nothing, but they share a common and consequential limitation: they treat insecure technology as a given and try to manage risk within it.

> ***Operators are absorbing the cost and taxpayers are funding the remediation. Manufacturers are retaining the revenue. This is a policy issue that state action can meaningfully influence.***

Two specific contract vehicles give the Commonwealth immediate leverage it has not yet fully used. The first is the Commonwealth IT Terms and Conditions, jointly administered by EOTSS, the Operational Services Division (OSD), the Office of Administration and Finance, and the Comptroller's Office, which govern all executive branch technology purchases. These terms were updated in July 2025 but the update addresses operational warranties such as malware-free deliverables and vendor personnel vetting. It does not establish affirmative Secure by Design requirements such as mandating multifactor authentication enabled by default, prohibition of default passwords, requirements for default-on logging or machine-readable audit trails, and vendor disclosure obligations for known vulnerability classes.

The second vehicle is OSD's IT Statewide Contracts, which set terms for technology products and services purchased across agencies and municipalities. These contracts currently contain little language of the kind outlined in CISA's **Secure by Demand guidance, such as requirements that vendors demonstrate MFA defaults, provide logging at no extra cost, or disclose their software bill of materials.** Updating both vehicles to incorporate a baseline Secure by Design standard would not require new legislation; EOTSS and OSD have the existing authority to act.

A third lever exists and is equally unused: the cybersecurity grant funds that EOPSS's Office of Grants and Research administers to municipalities and state agencies under the federal State and Local Cybersecurity Grant Program. The Commonwealth currently distributes these funds with priorities focused on MFA adoption, dot-gov migration, and cybersecurity awareness training—all worthwhile, but none constituting a Secure by Design condition on the technology purchases those grants enable. EOPSS has the authority to attach procurement security requirements to grant awards. It has not done so. The result is that Commonwealth funding flows to municipalities without any requirement that the technology purchased with it meet a baseline security standard, allowing state dollars to subsidize the same insecure-by-default products that create the infrastructure exposure described above.

> ***It would require a policy decision to treat software security as a procurement criterion rather than a post-purchase remediation problem.***

In the longer term, Massachusetts could also explore liability frameworks for software sold into critical infrastructure, establishing that manufacturers bear some responsibility for foreseeable harm caused by insecure products within existing state consumer protection and product liability authorities. The federal government has moved slowly on this question. States have acted before on product liability in the absence of federal leadership, and Massachusetts has a history of doing exactly that.

Developing both procurement standards and a liability framework and coordinating that effort across the New England region represents among the highest-leverage actions available to the Commonwealth. Doing so does not require waiting for federal action; instead, it requires deciding that the current distribution of risk is unacceptable and acting accordingly.

CHALLENGE IV — LARGE-SCALE TECHNOLOGY INVESTMENTS ARE OUTPACING SAFETY STRATEGY

Massachusetts is making strong bets on emerging technology, particularly in AI and the clean energy transition, that are proceeding without a parallel framework to ensure the technology underlying them is secure by design.

Artificial intelligence.

AI is being adopted across Commonwealth operations with growing speed, aided by the MassTech AI Hub. However, the Commonwealth currently lacks procurement standards to benchmark AI capabilities against public safety and security criteria. The default assumption is that security can be addressed after deployment, but as we have seen time after time, it cannot. Between ever-growing AI-generated insecure code, agents sitting atop insecure software, and tools to find (but not yet patch) exponentially more vulnerabilities, the risks are compounding without compensatory safety frameworks. The federal government's recent AI security actions compound rather than resolve this gap. The June 2026 executive order on AI security focuses on vetting national security risks of frontier models (through voluntary developer participation) and on hardening federal government systems; it does not establish software security requirements for AI products entering the broader market, and the December 2025 executive order preempting state AI laws actively constrains the Commonwealth's ability to fill that void unilaterally through regulation. Massachusetts cannot wait for a federal framework that is oriented toward AI dominance rather than AI safety.

Clean energy transition.

Massachusetts' ambitious clean energy buildout which calls for distributed generation, smart grid infrastructure, and electrification at scale will be underpinned by software and connected devices that are, by default, not built securely. The same insecure-by-default products that enabled Volt Typhoon's intrusions into water utilities are already embedded in energy infrastructure. Scaling that infrastructure without upstream security requirements risks repeating a familiar mistake at greater scale. During my time at CISA, we developed a strategy and implementation plan with the Biden White House on implementing Secure by Design principles for securing the technology underpinning the green energy transition. The Trump Administration has not moved forward with that plan, but Massachusetts could adopt aspects of it.[1]

[1] Biden-Harris Administration Energy Modernization Cybersecurity Implementation Plan: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/12/Energy-Modernization-Cybersecurity-Implementation-Plan.pdf

CHALLENGE V — NO MECHANISM FOR LEARNING FROM CYBER FAILURES AT SCALE

When a critical infrastructure operator is compromised, the immediate focus is containment, recovery, and restoration of service, which is an appropriate response. But the information contained in that failure, e.g., which vulnerabilities were exploited, what design decisions made the system susceptible, and what detection gaps allowed the intrusion to persist is rarely recorded to drive policy or upstream technical change.

1,793

of 2,164 breach attributions: "unknown or other" (2024)

938

of 1,526 breach attributions: "system intrusions" (2024)

86

average days to breach discovery — healthcare (2024)

The May 2026 joint report by the Office of Civil Affairs and Business Regulation (OCABR) and MassCyberCenter, which represents the Commonwealth's most rigorous analysis of breach data to date, makes this gap concrete. Of 1,526 breaches analyzed, 938 were system intrusions and 727 involved internet-facing vulnerabilities, but those specific vulnerabilities were not captured by the form. Almost certainly, most of these defects' underlying weakness classes are defects the development community has known how to prevent for decades. Yet the Chapter 93H reporting form that feeds this analysis does not collect vendor names, product versions, or vulnerability classes. As I noted in a formal response submitted to OCABR and MassCyberCenter, we can improve the form to collect better data to drive understanding and, in turn, better policy. I submitted my assessment of this report to both MassCyber and OCABR in May 2026.

CIRCIA and the Federal Gap

The federal government was supposed to address part of this through the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). The final rule has been delayed and its scope remains unsettled. Massachusetts and its neighbors cannot build their safety architecture around a federal reporting framework that does not yet exist in final form and may, when finalized, be designed primarily as a compliance and law enforcement mechanism rather than a safety and learning one. A compliance frame creates incentives to minimize disclosure and maximize legal protection. A safety frame modeled on aviation's reporting system, which transformed an industry not by punishing failure but by systematically learning from it creates incentives to share, because participants understand that the data makes everyone safer. At the same time, no single state can build a meaningful learning system alone. The dataset is too small, the infrastructure dependencies too regional, and the policy levers too interconnected; therefore, a New England regional approach is both the practical and the principled path forward.

RECOMMENDED ACTIONS

The Commonwealth need not build an entirely new system. The following steps would align existing authorities, close critical gaps, and establish a foundation for longer-term capability.

1. Establish a state-level cyber safety function.

This body should assess systemic cyber risk across sectors, advise the Governor and legislature on infrastructure exposure, and coordinate action across agencies, municipalities, and regulators. It should be explicitly distinct from incident response, oriented toward risk reduction and prevention, with a mandate to

advise on technology policy from a public safety standpoint including AI adoption, clean energy infrastructure, and critical systems procurement. EOPSS is the logical institutional anchor for this function: its existing authority over emergency management, law enforcement coordination, and physical infrastructure protection makes it the appropriate home for a cyber safety capacity that bridges the gap between technology governance and public safety. Locating this function within EOPSS would also leverage existing interagency relationships with MEMA, the Fusion Center, and sector regulators, rather than requiring a new standalone entity.

2. Develop a statewide view of infrastructure exposure.

Aggregate data from regulators, municipalities, and federal partners to identify common points of vulnerability and prioritize high-risk systems: internet-exposed edge devices, end-of-life operational technology, and systems undergoing transition as part of the clean energy buildout.

3. Leverage procurement and funding as market-shaping tools.

Direct EOTSS and OSD to update the Commonwealth IT Terms and Conditions and IT Statewide Contracts to incorporate a Secure by Design baseline, **including MFA enabled by default, no default passwords, default-on logging at no extra cost, software bill of materials disclosure, and lifecycle support commitments.** These vehicles govern all executive branch technology purchasing, so updating them requires no new legislation. Direct EOPSS's Office of Grants and Research to attach equivalent Secure by Design conditions to cybersecurity grant awards under the State and Local Cybersecurity Grant Program. EOPSS already has authority to set grant conditions; doing so would ensure that Commonwealth funding does not subsidize the purchase of insecure-by-default technology at the municipal level, and would extend market pressure to vendors serving the broader public sector, not only executive branch agencies.

4. Integrate cyber risk into public safety and infrastructure policy.

Treat cyber risk alongside physical infrastructure resilience and emergency preparedness. EOPSS should be formally designated as the coordinating authority for cross-sector cyber-physical risk, with a mandate to align MEMA, sector regulators (DPU, DPH), IT governance (EOTSS), and economic development on a common threat picture. Scenario planning for simultaneous cyber and physical disruption—including Volt Typhoon-style attacks on water or energy systems affecting hospitals—should be a baseline expectation, not an exercise reserved for crisis moments.

5. Build a regional cyber safety reporting and learning system.

Massachusetts should work with New England partners to establish a voluntary cyber incident and vulnerability reporting system modeled on the aviation safety reporting framework. The Massachusetts Fusion Center's existing cyber infrastructure and interstate relationships provide a foundation to build from.

6. Explore a state-level liability framework for critical infrastructure software.

The Commonwealth should examine legislation establishing meaningful legal liability for technology manufacturers whose insecure products cause foreseeable harm to critical infrastructure operators or the public. Safe harbor provisions for vendors who demonstrably meet Secure by Design standards could reward good actors while raising the market floor. This is among the most structurally significant actions available to the Commonwealth.

7. Build regional coordination capacity across New England.

Establish a regional cybersecurity coordination mechanism focused on shared threat and exposure awareness, coordinated technology procurement standards, and mutual aid frameworks for significant cyber incidents. This does not require federal permission or funding. It requires one state to decide to lead. Massachusetts is well positioned to be that state.

8. Establish procurement and safety standards for emerging technology.

Develop procurement standards specific to AI and clean energy domains, including security benchmarks for AI systems deployed in public-facing or critical functions, and baseline security requirements for connected infrastructure in the clean energy buildout. The window to establish these standards before the technology is entrenched is open now. It will not remain open indefinitely.

A note on sequencing: executive action first, legislation to follow.

The eight recommendations above are deliberately scoped to what the executive branch can do within existing authority. The Massachusetts General Court's Joint Committee on Advanced Information Technology, the Internet and Cybersecurity is active but has not yet engaged with software product accountability as a legislative priority. The legislative action that is both feasible and high-value in the near term is narrow: a statutory requirement that OCABR's annual breach report capture vendor and vulnerability class data. That is a data collection mandate, defensible entirely as consumer protection, and it builds the public record on which a future software liability argument rests.

CONCLUSION

Massachusetts has the institutional strength, technical expertise, and convening authority to lead in this space. What is currently absent is a coordinated strategy and a designated place within government where this problem is owned. The executive branch actions recommended here do not require waiting for the legislature. They require deciding that the current distribution of risk—in which software vendors externalize the cost of insecure products onto operators, municipalities, and residents while bearing none of it themselves—is unacceptable, and acting accordingly within existing authority.

> ***Software is in its 1965 moment. The Commonwealth has the data, the regulatory infrastructure, the historical precedent, and the executive authority to act.***

Massachusetts has led this story before—on auto safety, on consumer protection, on data breach notification. I welcome the opportunity to brief your team or support further development of these recommendations, including on legislative strategy when the moment is right.

ABOUT THE AUTHOR

Lauren Zabierek is a national security strategist with more than two decades of experience working at the intersection of cybersecurity, technology, national security, and public policy. Her background spans the U.S. military, the intelligence community (including three combat deployments to Afghanistan), and the private sector, where she worked at Recorded Future focusing on nation-state cyber threats and their real-world infrastructure impacts.

She most recently served as a Senior Advisor at the Cybersecurity and Infrastructure Security Agency (CISA), where she helped lead the Secure by Design initiative—an effort to shift responsibility for cybersecurity toward technology manufacturers and address systemic sources of risk. Prior to that, she directed the Cyber Project at the Belfer Center for Science and International Affairs at Harvard Kennedy School.

She is currently a Senior Advisor with CAS Strategies and co-founder and CEO of the Software Safety Institute, a 501(c)(3) public-interest nonprofit dedicated to advancing independent research and policy to improve software safety and resilience.

Lauren Zabierek

LZX Consulting | CAS Strategies | Co-Founder & CEO, Software Safety Institute | Foundation Layer

lauren@lzxconsulting.com | www.laurenzabierek.com