POLICY MEMORANDUM

Preparing Massachusetts for Systemic Cyber Risk: Volt Typhoon, Critical Infrastructure, and the Role of EOPSS

TO: The Honorable Gina Kwon, Secretary, Executive Office of Public Safety and Security
FROM: Lauren Zabierek, CEO & Co-Founder, Software Safety Institute | Former Senior Advisor, CISA
DATE: June 2026

PURPOSE

This memorandum provides an assessment of nation-state cyber threats to Massachusetts critical infrastructure, specifically the Volt and Salt Typhoon campaigns attributed to the People's Republic of China, and recommends concrete actions the Executive Office of Public Safety and Security (EOPSS) is positioned to take within its existing authority. It draws on my work at the Cybersecurity and Infrastructure Security Agency (CISA), where I co-led the Secure by Design initiative, and on the ongoing research and policy work of the Software Safety Institute (SSI), the 501(c)(3) public-interest nonprofit I co-founded to advance software manufacturer accountability as a matter of public safety.[1,2]

I am also sharing context from UnDisruptable27, an initiative of the Institute for Security and Technology (IST) focused on community-level resilience against infrastructure disruption with which I've worked alongside over the last year.[3] I am not writing on their behalf, but their work illuminates the current challenges with Massachusetts' preparedness this memo addresses and complements the upstream policy recommendations below.

THE THREAT: VOLT & SALT TYPHOON AND MASSACHUSETTS EXPOSURE

Volt Typhoon is a state-sponsored cyber campaign attributed to the People's Republic of China (PRC) with a documented mission to pre-position inside U.S. critical infrastructure, specifically in water, energy, transportation, and communications in order to enable disruption should the United States intervene militarily in a conflict over Taiwan.[4] The U.S. government (CISA, FBI, NSA) have warned that this campaign in civilian critical infrastructure is not consistent with nation-state espionage, and assess that it is instead preparation for disruption.[5] Its sister campaign, Salt Typhoon has compromised telecommunications systems across the U.S. and globally, and is assessed to be designed to disrupt communications during a Volt Typhoon-type disruption.[6,7]

[1] Secure by Design | CISA
[2] https://www.softwaresafety.org/
[3] UnDisruptable27, is an initiative of the Institute for Security and Technology (IST, a technology think tank) which focuses on the downstream consequence of the upstream policy failure SSI addresses. Led by Joshua Corman with support from Craig Newmark Philanthropies, UnDisruptable27 works directly with water utilities, hospital systems, and communities to build physical and operational resilience against cascading infrastructure disruption through preparing communities for worst-case scenarios before 2027 using the Idaho National Lab's Cyber Informed Engineering guidance to mitigate the worst consequences of an attack. UnDisruptable27's main insight is that the best near-term mitigations for many of these threats are physical and operational, not digital, and they include storing water, establishing manual backup and isolation procedures, and pre-staging mutual aid relationships. As Josh Corman says, "no water, no hospitals, no kidding." Hospitals and emergency medical care is critically dependent upon water; within a few hours of disruption, patients must be diverted to other locations to receive care. It also means no fire response capability, drinking water disruption, and no schools. These are just some examples of cascading, devastating effects, and the consequences are deadly.
[4] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
[5] The CCP Cyber Threat to the American Homeland and National Security. House Select Committee on China
The CCP Cyber Threat to the American Homeland and National Security
[6] Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System | CISA
[7] Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications | Congress.gov

The campaign's method of initial access is also noteworthy and something we can address in the long-term with concerted action on software safety: actors exploited well-known, preventable vulnerabilities in commodity edge devices, e.g., the firewalls and routers deployed at the perimeter of small and mid-sized utilities and municipalities.[8] These devices, despite their use in cybersecurity, are insecure by design and by default. They reached the market without meaningful security requirements because there is no legal liability to account for the harms they cause, nor are they governed by mandatory safety standards.[9] Once inside, actors are "living off the land," using legitimate system activities to avoid detection while establishing persistent access to the controls for our water (and energy, communications, and transportations) systems. U.S. officials have testified that the PRC intends to be capable of disrupting domestic infrastructure by 2027, though other estimates put this action at 2028 or 2029.[10] Regardless of the timeline and the nation and/or actor (because Volt Typhoon is not the only one that threatens our lifeline critical infrastructure), the threat is real and it is here, and we must take concerted, coordinated action to prepare for disruption and mitigate its consequences. Because of the scale of the compromise, its persistent, low-observable tradecraft, and the fact that security logging and retention capabilities are frequently restricted to premium software licenses which limits organizations' ability to detect sophisticated intrusions, there are likely many infrastructure entities that don't even know they're compromised. For this threat, incident response alone is insufficient and comprehensive threat hunting, eradication, and recovery across all potentially affected infrastructure owners is not currently feasible. It's expensive, time-consuming, and there are limited numbers of firms that do this work. Moreover, the Cybersecurity and Infrastructure Agency (CISA), which has historically provided this assistance, has experienced significant personnel departures and budgetary constraints over the past year, limiting its capacity to provide this support at national scale.[11]

While Massachusetts has built important cybersecurity capabilities and existing emergency management functions, none of them alone is designed to prepare for or coordinate response to and recovery from this threat. The existing mechanisms for Executive Branch continuity planning and single-sector incident response do not reach the municipal utilities, hospitals, and private infrastructure operators that are Volt Typhoon's actual targets. No entity in Massachusetts has the mandate, the visibility, or the authority to coordinate preparedness across that full range of institutions, and so the recommendations in this memo are scoped to what EOPSS can do now, within existing authority. The most important recommendation is also the most straightforward: **designate a clearly accountable owner for systemic cyber risk within EOPSS, give it a cross-sector mandate, and task it with the necessary assessment and coordination work to keep Massachusetts safe.**

The Littleton Case

Littleton Electric Light and Water Department (LELWD), a small, under-resourced water and electric utility in Massachusetts is a confirmed target of Volt Typhoon. Discovered in 2023, the intrusion involved actors

[8] https://www.cisa.gov/resources-tools/resources/secure-design-alert-security-design-improvements-soho-device-manufacturers

[9] This is the focus of the Software Safety Institute, a public-interest 501(c)(3) nonprofit established here in Massachusetts founded as a direct continuation of Secure by Design and to advance the principle that software insecurity is a product safety failure requiring manufacturer accountability, not solely operator remediation. At CISA, that work produced the Secure by Design whitepaper with principles and approaches, a Secure by Design pledge, and Secure by Demand guidance, which was a framework giving public and private sector buyers the language and criteria to require security as a baseline condition of doing business with technology vendors. SSI now seeks to carry that framework forward at the state level: developing procurement standards for state and federal acquisition, analyzing liability frameworks for insecure software sold into critical infrastructure, and producing the research and policy analysis that supports legislative and regulatory action. 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. I have already submitted policy analysis to the Governor's office and to OCABR on these issues, and we hope to engage directly with Commonwealth agencies on standards that would require vendors to meet Secure by Design baselines as a condition of doing business with Massachusetts (see both the "Massachusetts Cyber Risk Memo to the Governor" I sent to Constituent Services on June 8, 2026 and the "Lauren Zabierek response to the MassCyber Data Breach Report" sent to MassCyber and OCABR on May 14, 2026). The EOTSS IT Terms and Conditions and OSD statewide contracts remain an immediate opportunity: updating them to require MFA by default, prohibit default passwords, and mandate logging at no extra cost would not require new legislation and would meaningfully raise the security floor for technology purchased across the executive branch and by municipalities. I have also recommended establishing software liability, as the software industry currently disclaims liability for the harms created by their insecure products through its end user license agreements.

[10] The CCP Cyber Threat to the American Homeland and National Security. House Select Committee on China
The CCP Cyber Threat to the American Homeland and National Security

[11] CISA's vulnerability scans, field support on chopping block in Trump budget | Cybersecurity Dive

compromising the utility's network and "living off the land," to passively observe and pre-position to disrupt water and energy operations should the United States intervene militarily in a conflict over Taiwan.[12] 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 in Boston and Cambridge, yet faces this threat largely alone, illustrates a stark gap in how we create and manage technological risk.

Littleton is one of hundreds of known Volt Typhoon compromises across the United States and Guam.[13] 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.[14] 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. LELWD is not unique in this regard; Massachusetts has several similarly sized and similarly exposed water, electric, and wastewater utilities. Many serve communities that also host hospitals, emergency services, and the infrastructure that supports them. A coordinated Volt Typhoon-style disruption affecting water and power simultaneously, especially in a scenario involving hospital dependency on both would be a public safety emergency, not merely a cybersecurity incident. This is the work of UnDisruptable27, led by my colleague Josh Corman–it's meant to work with municipalities across the United States that have both a water utility and a hospital and prepare them to operate in isolation, without communications, and without the internet.[15,16]

SYSTEMIC CYBER RISK

Volt and Salt Typhoon (and similar nation state and cyber criminal activity targeting civilian critical infrastructure) pose a systemic cyber risk problem. Whereas organizational cyber risk arises within a single institution, systemic cyber risk arises when independently managed infrastructure systems become interdependent; i.e., when the compromise or failure of one cascades into others and has significant harmful effects upon the public. A water utility's disruption becomes a hospital's crisis and public safety emergency, and a communications outage compounds a power disruption. Managing this class of risk requires visibility across organizations and requires someone to hold the cross-sector picture, assess interdependencies, and coordinate preparedness before a crisis makes coordination impossible. The Commonwealth routinely assigns ownership for hazards that span jurisdictions, whether hurricanes, hazardous materials, or pandemics. Cyber-physical infrastructure disruption is now a hazard of the same character and warrants the same institutional clarity and action.

I made this point to make the case for what kind of institution is needed. Better incident response *within* individual agencies will not address systemic risk, and neither will improved cybersecurity within state government IT. What is required is a body with visibility and coordination authority that extends beyond any single agency or sector, one positioned to see the full range of infrastructure at risk and to act across the boundaries that currently separate the entities responsible for it. Cybersecurity is no longer solely an information technology problem; it is a public safety, emergency management, and infrastructure resilience problem. Software has become infrastructure, and the systems controlling water treatment, power distribution, and hospital operations run on software built without meaningful security requirements or standards, can result in infrastructure failures with public safety consequences. That is the domain of emergency management, and it is why this is an EOPSS problem.

[12] China is hacking America's critical infrastructure, former NSA and retired Gen. Tim Haugh warns - CBS News
[13] LELWD Publicizes Case Study on Foreign Hackers Targeting U.S. Utilities
[14] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA
[15] Testimony: Research-Driven Resilience: Applying Science to Secure U.S. Water Systems from Cyber Threats
[16] UnDisruptable27 Archives - Institute for Security and Technology

EXISTING STRUCTURES AND SHORTFALL

Massachusetts has one of the stronger state cybersecurity ecosystems in the country and should be recognized for its investments, along with the hard work and dedication of all those who serve in these roles across the state, its departments, and its 351 municipalities. The Executive Office of Technology Security Services (EOTSS) operates a Commonwealth Security Operations Center and administers the MA Cyber Incident Response Team (MA-CIRT). MassCyber Center provides municipal support and training. The Massachusetts Fusion Center maintains cyber infrastructure and interstate relationships. These organizations are structured around specific missions, agencies, and sectors, while Volt Typhoon targets infrastructure that spans organizational, ownership, and jurisdictional boundaries. Specifically, they are incident-response oriented, not designed for persistent pre-positioned threats that may not be detectable as "incidents" until the moment of disruption. They also operate within existing technology as given, without authority or mechanism to assess the aggregate exposure created by insecure-by-default products deployed across the Commonwealth's infrastructure.

The result is an asymmetry between the cybersecurity capabilities that exist and the state's ability to understand systemic cyber risk across critical infrastructure. Addressing this does not necessarily require creating a new institution if one exists presently; but it does require assigning clear responsibility for assessing cross-sector risk, identifying dependencies, providing decision-makers with a comprehensive view of statewide exposure, and coordinating preparation and recovery within EOPSS.

Current MEMA and COOP Documents

Executive Order #490 requires Executive Branch agencies to maintain Continuity of Operations Plans (COOPs) and submit them to the Massachusetts Emergency Management Agency (MEMA).[17] The requirement does not extend to municipalities or privately operated critical infrastructure. Although many of these entities maintain continuity or emergency plans pursuant to sector-specific federal or state requirements, Massachusetts has no comparable statewide *preparedness* framework that establishes common planning expectations across these entities, provides the Commonwealth with routine visibility into those plans, or supports coordinated assessment of cross-sector dependencies before a crisis occurs. As a result, continuity planning is largely organized within individual organizations rather than across the interconnected infrastructure systems on which the Commonwealth depends. LELWD is a municipal utility, the hospitals that depend on its water are private or quasi-public institutions, and the electric distribution assets most exposed to campaigns such as Volt Typhoon are operated by a mix of municipal and investor-owned utilities. The Commonwealth's mandatory continuity planning framework therefore applies primarily to state government, while much of the infrastructure whose disruption would have the greatest public safety consequences lies outside that framework, without standardized reporting, coordinated assessment of interdependencies, or a mechanism for statewide visibility into preparedness.

Chemical hazard preparedness in Massachusetts provides a useful model. The State Emergency Response Commission (SERC), established under the federal Emergency Planning and Community Right-to-Know Act (EPCRA), reaches private industrial facilities and municipalities through mandatory Tier II chemical reporting requirements.[18] It has a statutory basis, designated leadership, Local Emergency Planning Committees that convene across the Commonwealth, and defined relationships among state agencies, local governments, emergency responders, and private industry. The result is a standing governance structure that provides the Commonwealth with visibility into reportable chemical hazards across sectors, rather than only within state government. No comparable statutory framework exists for cyber risk. Executive Branch agencies submit COOPs independently, and MEMA receives those plans, but no statewide mechanism provides comparable visibility into the cyber preparedness, interdependencies, or systemic risk exposure of municipal utilities, hospitals, or privately operated critical infrastructure.

[17] Continuity and Safety Planning Guidance | Mass.gov
[18] Massachusetts State Emergency Response Commission (SERC) | Mass.gov

The Commonwealth's sector regulators maintain the relationships that the COOP framework requires. MassDEP oversees public water systems, including municipal utilities; the Department of Public Utilities regulates investor-owned electric and gas utilities; and the Department of Public Health maintains longstanding relationships with the hospital systems that depend on both. Each agency also has cybersecurity responsibilities within its own regulatory domain. However, no entity is charged with assessing systemic cyber risk across these sectors or coordinating preparedness for the interdependent infrastructure on which the Commonwealth depends. What Massachusetts lacks is not additional planning within existing agencies; rather, it lacks a clearly designated owner for systemic cyber risk. Sector regulators oversee their respective industries, MEMA coordinates emergency management, and Executive Branch agencies maintain continuity plans, but no organization is responsible for identifying cross-sector cyber dependencies, coordinating preparedness among state agencies, municipalities, and private infrastructure operators, or providing EOPSS and the Governor with a comprehensive assessment of statewide cyber resilience before a disruption occurs.

ESF-17 (Cybersecurity)

ESF-17 (Cybersecurity) was added to the Commonwealth's Comprehensive Emergency Management Plan (CEMP) in 2018, alongside the other sixteen Massachusetts Emergency Support Functions (ESFs). Unlike those sixteen, which are individually published on MEMA's public CEMP page, ESF-17's annex is not publicly available, and I have not been able to identify its current content. However, based on a version I reviewed in 2021–2022 while working with Massachusetts water and wastewater cybersecurity stakeholders, the annex appeared out of date, listing NCCIC rather than CISA as its federal counterpart and omitting several state agencies with responsibility for critical infrastructure sectors in Massachusetts.[19] Whether its current inaccessibility reflects its sensitivity, its age, or simply a publishing oversight, the result is that there is no public basis to assess whether ESF-17 reflects the current threat environment, let alone the one Massachusetts will face from a Volt Typhoon-style threat, or similar threats in the future.

The CEMP publicly specifies that ESF-17 "provides a **framework** for coordination and cooperation **across agencies** before, during, and after a cyber-related emergency or disaster affecting, or having the potential to affect, the Commonwealth in a significant manner" (emphasis added by the author). It is unclear the capacity for coordination with municipalities, public and private sector critical infrastructure entities, the federal government, MA-CIRT, and MA Fusion Center, nor is it clear who leads such an effort. The CEMP's other sixteen ESFs are organized as single-hazard, single-sector incident annexes, e.g., Search and Rescue, Hazardous Materials, Energy, which are each activated to coordinate response to a discrete event within its own domain. ESF-17 must be designed to prepare for, manage, and mitigate a coordinated, pre-positioned campaign disrupting water, energy, and healthcare delivery systems simultaneously, where no single ESF owns the response and effective action depends on coordination across several at once.

Whether ESF-17 needs to be substantially updated or rewritten outright is a determination only EOPSS and MEMA can make with access to the current document. An effective ESF-17 will depend on preparation that does not appear to exist (at least from the outside): a cross-sector exposure assessment identifying which water, energy, and health systems are most likely targets; pre-established coordination protocols between ESF-17, ESF-12 (Energy), and ESF-8 (Public Health and Medical Services) for a simultaneous-disruption scenario; processes and protocols for mitigating the consequences of disruption; and exercises that test those protocols before they are needed. At the same time, it is clear from our research on the issues that more players need to be in the room: from public and private sector critical infrastructure operators, original equipment manufacturers, systems integrators, incident response/threat intelligence/managed security/and recovery firms, as well as the state government entities responsible for the sectors and municipal leaders.

National Guard

The Massachusetts National Guard has important cyber capacity: it hosts Cyber Yankee, a regional exercise evaluating whole-of-government response to cyber incidents affecting critical infrastructure, and has a Massachusetts-based cyber intelligence, surveillance, and reconnaissance unit. However, relying on the

[19] During my tenure as Executive Director of the Cyber Project at Harvard Kennedy School's Belfer Center

National Guard as the primary response mechanism for a Volt Typhoon-style scenario involves significant risk. The scenario in which PRC actors activate pre-positioned access in U.S. infrastructure is one in which the United States is in or approaching armed conflict with China over Taiwan. That is the time when National Guard cyber units could reasonably be expected to be federalized under Title 10 and deployed in support of DoD's warfighting mission, thus removing them from state control and state availability at the moment of greatest domestic need. Massachusetts cannot plan its critical infrastructure resilience around assets that may not be there when the threat is activated.

STATE AND LOCAL ACTION IS ESSENTIAL

The Federal Vacuum and the State Imperative

The federal government remains an indispensable partner in critical infrastructure protection. The FBI, NSA, CISA, EPA, DOE, and HHS all have active roles, and their intelligence, technical resources, and sector expertise have not been replaced at the state level. But states can no longer assume that federal capacity alone will provide the sustained, on-the-ground support required for preparedness. CISA's regional cybersecurity advisors, i.e., the field staff who maintained direct relationships with utilities, municipalities, and critical infrastructure operators departed in significant numbers over the past year.[20] The resulting shortfalls in direct federal support fall hardest on the smaller, under-resourced operators most exposed to Volt Typhoon. Further, Executive Order 14239 ("Achieving Efficiency Through State and Local Preparedness," March 2025) reflects a new reality in which state, local, tribal, and territorial governments must assume greater responsibility for critical infrastructure protection without commensurate funding, staffing, or capacity building.[21] This makes state-level coordination not a supplement to federal action but rather an imperative. And coordination is the operative word because the Volt Typhoon scenario is not a single-agency problem.

Water disruption implicates public health and the inability for the Massachusetts financial and research and development sectors to operate (as well as schools and other daily functions). Power disruption implicates emergency management. Hospital dependency on both implicates life safety. Communications disruption impacts emergency management. Responding effectively and preparing before a response is required demands coordination across secretariats, across sector regulators, and across the municipalities that own and operate the infrastructure most at risk. Today, if the Governor asked for a single assessment of Massachusetts' cyber exposure across water, healthcare, energy, and communications infrastructure, no agency could provide it because no agency is responsible for producing it.

EOPSS is positioned to lead by convening across secretariats and the public and private sectors, establishing the preparedness mandate, and ensuring that Commonwealth funding does not subsidize the insecure technology that created this exposure in the first place.[22]

WHY EOPSS MUST DESIGNATE A CYBER RISK LEAD

Massachusetts has no shortage of agencies with some cybersecurity responsibilities. The question is which of them is positioned to own systemic cyber risk, and the answer points clearly to EOPSS. EOTSS secures *Commonwealth* IT infrastructure and administers MA-CIRT and its mandate is the state's own technology environment. MassCyber Center supports municipalities with training and resources, but it is an assistance organization, not a coordination authority. Sector regulators such as MassDEP, DPU, and DPH have deep expertise and existing relationships within their sectors, but none has a cross-sector view or an emergency management mandate. MEMA manages emergency response and receives COOP submissions, but it is structured around discrete emergency events, not persistent pre-positioned threats that may not produce a visible incident until the moment of activation.

[20] One-third of U.S. cyber agency CISA has left since Trump took office

[21] Achieving Efficiency Through State and Local Preparedness – The White House

[22] See the "Massachusetts Cyber Risk Memo to the Governor" I sent to Constituent Services on June 8, 2026

EOPSS is the only institution positioned above all of those entities with both public safety responsibility and convening authority across secretariats. It oversees MEMA and the State Police Fusion Center; it can convene across secretariats on behalf of the Governor; it has existing relationships with sector agencies, municipalities, and federal partners; it administers federal homeland security grant programs that reach municipal infrastructure operators directly; and it is accountable to the Governor for public safety outcomes in a way that no single-sector agency is. Emergency management has always been about preparing for complex hazards that cross organizational boundaries before they happen. A coordinated cyber-physical disruption of water, energy, communications, and healthcare systems is the next manifestation of that mission.

RECOMMENDED ACTIONS FOR EOPSS

The following recommendations are scoped to what EOPSS can do within existing authority, without waiting for new legislation or federal action.

1. Establish a cross-sector cyber-physical preparedness and risk reduction function within EOPSS.

Designate a function that is staffed or initially convened as an interagency working group with an explicit mandate to **assess, prioritize, and communicate systemic cyber risk** to Massachusetts critical infrastructure, coordinate preparedness across MEMA, sector regulators, MassCyber, EOTSS, and municipalities, OT systems integrators, and to advise the Governor on infrastructure exposure.[23] This function should be explicitly distinct from incident response and oriented toward prevention and resilience.

a. This function within EOPSS **should also have an explicit mandate to reduce systemic cyber risk** to Massachusetts critical infrastructure. This might look like a **statewide Software Safety Initiative for Critical Infrastructure** in partnership with EOTSS, MassCyber, sector regulators, universities, nonprofits, and industry, that works to identify and eliminate common sources of software risk, developing statewide software safety priorities, coordinating risk reduction across sectors, and recommending changes to procurement, regulation, grantmaking, and public-private partnerships that eliminate common classes of vulnerability. This would make Massachusetts a national leader in this domain.

2. Initiate a statewide infrastructure exposure assessment.

Working with EOTSS, MassCyber Center, sector regulators, and the Fusion Center, EOPSS should develop a statewide picture of infrastructure exposure through internet-exposed edge devices, end-of-life operational technology, hospital dependency mapping, and systems most likely to appear in a Volt Typhoon-style target set. This assessment need not be exhaustive to be useful. A prioritized view of high-risk systems, particularly water utilities, hospitals, and energy distribution nodes, would inform both preparedness planning and procurement standards.

3. Review and revise ESF-17

EOPSS and MEMA should conduct a review of ESF-17's current annex to determine whether it reflects the current threat environment and whether it is structurally capable of coordinating a multi-sector, simultaneous-disruption response. Based on that review, ESF-17 should be updated or rewritten to name the relevant state and federal counterparts for each critical infrastructure sector; establish formal coordination protocols with ESF-12 and ESF-8 at a minimum; define the roles of municipal operators and private sector entities in a cyber-physical emergency; identify the necessary private sector firms (systems integrators, OEMs, incident response and recovery entities) and provide a framework for the pre-crisis assessment and information sharing that incident-response-only structures do not support. The revised annex should be exercised before it is needed.

[23] Of note, we include the systems integrators here because they represent either the obstacle or point of leverage during a crisis because of their contracts; having them in the room is vital for preparation and coordination.

4. Formally align EOPSS cyber preparedness with New England regional partners.

Volt and Salt Typhoon do not respect state boundaries. A disruption scenario affecting Littleton's water system has implications for adjacent communities, mutual aid networks, and regional emergency response. EOPSS should work with counterparts in neighboring states to establish shared threat awareness, coordinated preparedness exercises, and mutual aid frameworks specific to cyber-physical incidents.

5. Formally designate state sector cyber risk leads within existing regulatory agencies.

At the federal level, Sector Risk Management Agencies (SRMAs) are designated leads for cybersecurity coordination within each critical infrastructure sector, to include EPA for water, DOE for energy, HHS for healthcare. Massachusetts has the state-level regulatory counterparts to each: MassDEP for water, the Department of Public Utilities (DPU) for energy, and the Department of Public Health (DPH) for healthcare.[24] EOPSS should work with the Governor's office to formally designate MassDEP, DPU, and DPH as state sector cyber risk leads for their respective sectors at a minimum with defined responsibilities to maintain an active relationship with their federal SRMA counterpart, receive and translate sector-specific threat information, participate in cross-sector preparedness planning under EOPSS coordination, and report on sector exposure as part of a statewide infrastructure picture. This is the state-level functional equivalent of the federal SRMA structure, achievable within existing agency authority and without new legislation. It also directly supports the ESF-8 and ESF-12 coordination recommended above: if DPH and DPU carry a formal sector cyber risk role, they become the natural counterparts for cross-ESF planning rather than peripheral participants who must be convened ad hoc in a crisis.

6. Leverage EOPSS's grant authority to attach Secure by Design conditions to cybersecurity awards.

EOPSS's Office of Grants and Research administers federal State and Local Cybersecurity Grant Program (SLCGP) funds to municipalities and state agencies. Current grant conditions emphasize MFA adoption and awareness training which are worthwhile, but insufficient. EOPSS has the authority to attach procurement security requirements to these awards, requiring that technology purchased with Commonwealth-administered grant funds meet baseline Secure by Design standards such as MFA enabled by default, no default passwords, default-on logging, eliminating classes of defect, a vulnerability disclosure policy, and software bill of materials disclosure. This is among the highest-leverage actions available to EOPSS. It does not require new legislation, but it does require a policy decision to treat security as a condition of Commonwealth funding rather than an aspiration.

CONCLUSION

The threat Volt and Salt Typhoon poses to Massachusetts communities is neither theoretical, distant, primarily a technology problem, nor is it an isolated incident (as other nation states and cyber criminal groups continue to probe for weaknesses and hold our critical services for ransom). It is a public safety problem with a short horizon, and Littleton is evidence that it is already here. EOPSS has the authority, the institutional relationships, and the interagency position to lead the Commonwealth's response in ways that no other body can. Massachusetts already possesses many of the institutions required to meet this challenge. The state must assign clear ownership for systemic cyber risk before a crisis forces that decision under far less favorable circumstances.

I would welcome the opportunity to brief you or your team on any aspect of this analysis, including the threat picture, SSI's policy recommendations, UnDisruptable27's community resilience work, or the specific procurement and preparedness actions outlined above. I am also happy to share the full policy memorandum

[24] The federal government designated sector risk management agencies (SRMAs) as part of its Presidential Policy Directive-21 (PPD-21). PPD-41 established the roles of lead federal agencies for threat response, asset response, and intelligence support during significant cyber incidents. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

I prepared for the Governor's office, which develops the Commonwealth-wide case in greater detail or the response to the MassCyber/OCABR Data Breach report.

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. Air Force, the civilian 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 after graduating from there with an MPA in 2019.

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.

With respect,
Lauren

Lauren Zabierek
CEO & Co-Founder, Software Safety Institute | Senior Advisor, CAS Strategies | President, LZX Consulting
lauren@lzxconsulting.com | www.laurenzabierek.com