Testimony of William Francis Galvin
Secretary of the Commonwealth of Massachusetts

Subcommittee on National Security
May 22, 2019

Thank you Chairman Lynch, Ranking Committee Member Hice, and distinguished committee members of the Subcommittee on National Security for inviting me to testify today on the safety and security of the nation's election infrastructure and the ongoing misinformation attempts to influence public opinion and trust in our election system. My name is Bill Galvin and I have been the Secretary of the Commonwealth since 1995. During my tenure as Secretary, I have worked hard to ensure elections in Massachusetts are fair, honest and accurate. My office successfully implemented a statewide database after passage of the National Voter Registration Act (NVRA) and has continued to make improvements to implement state and federal laws, including the Help America Vote Act (HAVA). In recent years, however, new challenges have emerged. I do not need to tell this distinguished Committee about the real threat that we face, and the importance of protecting our election infrastructure from malicious attackers or the value of the public trust in our electoral system given the nefarious efforts to thwart that public trust through disinformation. Instead, I will focus my testimony on the following four topics that are important to my office and the election community as a whole:

1. Strength through partnerships
2. Maintaining a consistent and efficient communication flow
3. The federal government's role
4. Predictable and sustainable funding

Before addressing each topic, I think it is important to note the differences in election administration throughout the country and how this leads to unique challenges. Unlike the majority of the country in which election administration is county-based, in Massachusetts and the rest of New England, as well as in Michigan and Wisconsin, elections are conducted on a municipal level with local election officials in each of the cities and towns. Local election officials in Massachusetts, most of whom have responsibilities beyond elections such as vital records and some of whom are part-time, have varying skills and expertise in security, and overall information technology knowledge as well as varying access to the resources likely available to county officials, such as on-site technical help.

Strength Through Partnerships

In Massachusetts, we have fostered many local, state and federal partnerships and leveraged the combined knowledge, talent and expertise to conduct tabletop exercises, produce incident response plans and formulate communication plans. Working with the Massachusetts statewide IT agency, State Police, and the Commonwealth Fusion Center has allowed us to develop an effective, cohesive and inclusive response to various possible scenarios both intentional and unintentional. These exercises have also fostered relationships that will allow us to bring to bear the combined resources of these entities in the event we have an incident response need. My organization is also partnered with DHS, FBI, the U.S. Election Assistance Commission (EAC) and the Belfer Center's Defending Digital Democracy program. Also, we are members of the Center for Internet Security (CIS), the Election Insfrastructure Information Sharing Information Sharing & Analysis Center (EI-ISAC), National Association of Secretaries of State (NASS), National Association of Election Directors (NASED), the Government Coordinating Council (GCC), and US Election Assistance Commission (EAC). These partnerships have been extremely critical in providing guidance, best practices, monitoring, alerts and intelligence to members of my Elections and IT staff.

We consider our local election officials among our partners, and we continue to expand our partnerships to include their IT staff and support, to the extent they have any. We continue to work with our local election officials to make sure we provide them with resources and support regarding election technology and general cyber-awareness. This is not a one-time effort; this is on-going work into the future.

Maintaining a Consistent and Efficient Communication Flow

Consistent and efficient communication must be bi-directional and follow prescribed points of contact. All of the federal agencies mentioned above must, in a timely manner, keep the individual states informed of suspected breaches, alerts, intelligence as well as the tactics, techniques and procedures (TTPs) used by our adversaries. In turn, the states need to provide outreach to city, town and county governments to increase awareness, training and mindfulness, as well as provide them assurance that the partners further up the communication chain are doing everything they can to protect the election infrastructure and thwart the efforts of those who wish to cause distrust and chaos in our democracy. Conversely, effective communication includes information reported by local governments about what they are seeing and are concerned about and should flow to the state and ultimately be passed to the appropriate federal entity or entities. We can all do a better job of reporting that vital information back up and down the communication chain. State Fusion Centers and the EI-ISAC have served as an ideal conduit for states to pass along the incidents and trepidations that local election staff are experiencing, from misinformation on social media to scanning and beyond. States need to ensure they are providing a vehicle for this up flow of communication

and concern and pass it up to the federal level. I believe it is critical that any information reported by a local jurisdiction is timely shared with the state election official as well. Additionally, this consistent and efficient communication chain should not be hindered by information siloes or delays and cannot be broken by circumventing any of the contact points. A breakdown of communication will occur if the states are left out. State election offices must remain the conduit for all federal and local correspondence.

The Federal Government's Role

The federal government, through DHS, must continue with information and intelligence sharing to the states, however more is needed in terms of guidelines and best practices for security of equipment, software and services. Many states already rely upon the voting equipment standards adopted by the EAC for certification of voting machines, but more needs to be done to make sure there are guidelines for other election technology, including electronic poll books, and requirements for vendors supplying equipment, the supply chain and software and related services. States need assurance that proper screening of vendors, sub-vendors and their employees is being done so that foreign or malicious influence of the equipment we utilize is not taking place. Security testing, like that done at the Idaho National Lab, of election-related equipment, software and services by the federal government should be addressed prior to market availability and reviews should be required regularly to address future vulnerabilities. Federal certifications need to address supply chain concerns of equipment and components that are not manufactured in the United States. The federal government must take a stronger regulatory authority role.

At my insistence, Massachusetts is a paper ballot state, providing a manual auditable process of all ballots. The election equipment that we use is publicly tested prior to each election – anyone interested can come and watch - and has no internet connectivity. Our post-election audits also ensure the confidence of voters. We have worked diligently to protect our election network infrastructure and we have isolated our voter database from the internet, regularly back-up the data and test that the back-up data is usable, and monitor logs for suspicious activity. This includes providing the network, equipment and technical support to local election officials in the 351 municipalities. Despite all the controls that we have implemented, the threat against our elections will not cease, and the malicious efforts will become increasingly difficult to identify and mitigate. Massachusetts would like to be able to rely on the federal government for assurances and guidelines as we look to replace voting equipment, make new purchases such as electronic poll books and replace or update election software. The federal government is better resourced and positioned to make sure all equipment, software and vendors in the election services marketplace consistently adhere to standards and ongoing certifications. However, these services must be expeditiously

implemented to avoid lapses in availability of technology and so as to avoid hindering development. The EAC's current voting system standards are outdated; they are structured such that they represent a moment in time. New standards need to be dynamic and easily updated so that the voting machines on the market can meet security best practices and voter and administrator expectations.

Additionally, the federal government needs to continue working with social media organizations and technology providers to identify and quash the deliberate misinformation campaigns, whatever the source. This includes promptly investigating misinformation reported by election officials. Instances of misinformation can be communicated up the chain, from local to state to federal entities allowing for and contributing to overall situational awareness and leveraging the federal government's weight to ensure the social media platforms, hosting companies and internet providers respond quickly and appropriately.

Predictable and Sustainable Funding

Election infrastructure is now deemed critical infrastructure and rightfully so. But assigning this designation of critical is not enough; it must be treated and subsequently funded as such. The recent HAVA funding has made it possible for Massachusetts to build in security controls and staff to monitor our infrastructure, but more needs to be done. Protecting our infrastructure from malicious actors who want to spread chaos and distrust is a chess game that requires focused concentration, planning and tremendous skill, all of which is costly. Technology costs incurred for security will be recurring, and funding will need to be maintained in order to continue to protect our democratic process. States are reluctant to take on tools, training and expert staff without knowing that their efforts are financially sustainable long-term.

Maintaining the confidence of the public and keeping out those who want to harm our democracy is worth the long-term investment. Moreover, this funding needs to be strategically shared down to the local jurisdictions. Massachusetts's 351 local municipalities have varied levels of knowledgeable, security-minded staff. My office has used HAVA funding to administer cyber security training to these local municipal staff, but there is more to do. Continued training, equipment replacements, software upgrades and implementation of security controls are all still needed at the state and local level. The original HAVA funding enabled us to assist municipalities in procuring new equipment, but that equipment is now nearing end-of-life. While we intend to use the newer HAVA funding to replace this aging equipment, unless there is an additional funding source provided in the future, we will likely be unable to provide financial assistance as the equipment procured now expires. Further, with the ever-changing world of technology, we are hopeful that new and innovative equipment will become

available, but additional funding would be necessary for future procurements. These and other needs require sustained funding as part of the election infrastructure we now call critical.

Conclusion

In closing, Massachusetts and my office are encouraged by what has been done by the federal government thus far. The recent HAVA funding, the continued efforts of our federal partners as well as individual efforts of states and local governments, and the designation of elections as a critical infrastructure has increased focus and attention on the security of elections, positioning us better than we were in 2016. 2018 was the most secure election in modern history, however, there is more work to do leading into 2020. The beginning of primary season is less than 10 months away; we need to move quickly to accelerate our efforts. If we all endeavor to work together through strong local, state and federal partnerships, share information through efficient and timely communications, lean on the federal agencies for guidance and certification of the private sector, and with predictable, sustainable and continued funding, we will protect our critical election infrastructure, ensure our democracy and keep those who mean us harm at bay. The alternative is unacceptable.

Thank you for the opportunity to provide this information to the Committee.