that

he online voter registration system used by voters to register and to request a ballot is necessarily connected to the internet with all of the associated risks. However, to minimize these risks, the voter registration website is hosted by a private firm in Annapolis that specializes in web hosting and web security. Data coming through the website is encrypted. The statewide voter registration database receiving the data sits on network that is not connected to the internet and is only accessible to SBE and the local boards of election. Transactions between the website and the voter registration database are regularly reviewed by staff for unusual or suspicious activity.

As a best practice, Ms. Charlson emphasized that SBE has recovery plans in the event of a serious cyber disruption. At the voting locations, staff protect back-up voter registration lists that are stored on laptops and in paper copy in case the electronic poll books fail. Likewise, if other equipment fails anywhere during an election, new equipment to be installed within two hours. (Repaired equipment is not recycled.) In the event that the electronic record of is suspect, paper ballots provide a physical record of the vote that can be hand-counted if necessary.

SBE exercises various scenarios from time to time to keep both state-level and local election staff ready for contingencies. Ms. Charlson noted, for example, that she and several other staff participated in a full day of challenging table-top exercises in Boston that were organized by the Belfer Center *Defending Democracy Project* at Harvard University.

1elfe(t (y)4(2s-8(e)0sifact P2uded7(e)4b(g DMC /2920(sica)5(l r)-8(e)4(c)4(ord o)-6(r6b4830085ps)-(e)4(lf)-26 0

user cannot proceed. Other backend checks are used to verify legitimate interactions with the system. There is no evidence that the voter registration database has been breached. Mr. Rauschecker (CHHS): Is there a role for the Council in election security? Ms. Charlson: There is a senate bill that would add SBE to the Council. Whether SBE is or is not on the Council, it is certainly willing to share information as appropriate to support the Council.

Subcommittee Reports

Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee, for both her and Mr. Blair Levin.

Senator Lee indicated that had introduced several bills that aligned with her recommendations of her subcommittee included in the July 2017 Activities Report:

SB 202 (Consumer Protection - Credit Report Security Freezes - Notice and Fees). This bill would extend the law passed last year (SB 525/HB 974) that provided for no charge for the first credit freeze. Specifically, for affected consumers, SB 202 would prohibit charges for any service related to a security freeze, including placement, temporary lift or removal and would allow parents and guardians similar rights with respect to their minors.

SB 376/HB 476 (Criminal Law - Crimes Involving Computers - Cyber Intrusion and Ransomware). This bill SB 287/HB 772 and is intended to accommodate concerns of the committees. Addressing cyber intrusion in general, the bill would identify ransomware as a crime and provide a right of private action for unauthorized computer and network intrusion.

SB 882 (Procurement Telecommunication and Computer Network Access Security). This bill has two purposes. In part, it
(IoT) devices to meet certain security requirements. In this respect, the bill is modelled on federal procurement regulations and aims to reduce the vulnerability of the state networks to breaches and disruption. In addition, the bill would restore net neutrality in light of the withdrawal of the FCC regulation that would have accomplished the same. The bill is similar

Mr. Markus Rauschecker for Professor Michael Greenberger, Chair, Critical Infrastructure Subcommittee

Mr. Rauschecker conveyed Professor Greenberger
meeting. He updated the Council on the repository for small- and medium-size businesses that is
http://www.umuc.edu/mdcybersecuritycouncil). He noted