CONCLUSION OF MORNING BUSINESS

The PRESIDING OFFICER. Morning business is closed.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to executive session to resume consideration of the following nomination, which the clerk will report.

The legislative clerk read the nomination of Peter Joseph Phipps, of Pennsylvania, to be United States Circuit Judge for the Third Circuit.

Mr. SCHUMER. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. WYDEN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

ELECTION SECURITY

Mr. WYDEN. Mr. President, I stand here this afternoon in a state of disbelief. Last Wednesday, my colleagues and I in the Congress were briefed on the state of election security in America.

I am prohibited from talking about the details of that classified briefing, but the message from my Republican colleagues after that elections security meeting was very clear: Nothing to see here. One Senator said it is clear the Federal Government is doing ''everything you can do.'' The top Republican on the House Homeland Security Committee said: ''I wouldn't say we've got a need for more election security legislation.'' A Member of the House Republican leadership said: ''The agencies have the tools they need, and I am confident they are addressing the threats.''

It is case closed for those Republicans—mission accomplished. My Republican colleagues were just so satisfied that the foundation of our democracy is in good hands. Election security is not a problem for those colleagues I just quoted.

It was to my enormous shock this weekend when I picked up my phone, and I read the following headline: ''Old Software makes new electoral systems ripe for hacking.''

Over the weekend, I said: Gosh, that just can't possibly be right. After all, my Republican colleagues said after the classified briefing that election security issues were in good shape. I just kept reading, and as it turns out, according to an exhaustive analysis by the Associated Press, the vast majority of 10,000 election jurisdictions nationwide use election management systems that run on old software that is soon going to be out of date and ripe for exploitation by hackers.

According to the Associated Press, Pennsylvania, Wisconsin, Michigan, Florida, Iowa, Indiana, Arizona, and North Carolina, among others, are all at risk. Even the State of Georgia, which just passed legislation to buy new voting machines, is on track to buy equipment that suffers from this significant cyber security weakness. Worse, two of the three largest voting machine companies, ES&S and Hart, don't make election systems that are free from this vulnerability. Many election officials will be buying election systems that will be out of date the moment they start using it.

I am reading this story, and I am thinking to myself: Maybe—just maybe—this Trump administration hasn't solved the election security issue.

Now, colleagues, I am being a little bit disingenuous here. I have actually known about this problem for some time. In fact, I wrote to the Election Assistance Commission about it because, of course, our elections weren't secure last week, and they sure as heck aren't secure this week. Anybody who says otherwise is either selling you a voting machine or simply has a malicious intent toward our elections.

Russia attacked our democracy on every front in 2016, including voter registration databases and election software vendors. I am a member of the Senate Intelligence Committee, and I can't talk about classified matters, but it is public record that there were attacks on our election infrastructure in 2018.

Our colleague Senator RUBIO of Florida even said that hackers were ''in a position'' to alter voter rolls in 2016. In April, the FBI Director said that 2018 was, ''just kind of a dress rehearsal for the big show in 2020.''

I will say, as I have been saying at home at townhall meetings across my home State, that in 2020 I believe the hostile foreign actors are going to make 2016 look like small potatoes, and I am not just talking about the Russians here.

What the Associated Press revealed this weekend should be chilling for anybody fighting to protect our elections from foreign interference, but it is certainly not the first indication Americans have gotten that our elections are vulnerable.

Last year, the journalist, Kim Zetter, and the New York Times reported that ES&S had installed remote access software and wireless modems in election equipment for years. I believe that is about the worst thing you can do in terms of election security in America, short of putting American ballot boxes on a Moscow street.

Special Counsel Robert Mueller revealed in his report that an election software vendor was actually hacked by Russia in the summer of 2016. The public still doesn't know enough about what happened there or what the government did to investigate. This is another area where I am seeking to excavate the facts. My colleagues, particularly my colleague from Minnesota, Senator KLOBUCHAR, and my colleague from Rhode Island, Senator REED, are doing the same.

VR Systems, the company Mr. Mueller was referring to, sold e-pollbooks to a county in North Carolina. I am talking now about the systems that workers used to check voters in at a precinct. It happened that several of the VR Systems e-pollbooks used by Durham County in North Carolina malfunctioned on election day in 2016. The problem was so bad that one precinct had to shut down completely for several hours.

Last month, I asked the FBI what happened; is anybody investigating? It sure looks like no Federal Agency has been out there looking at these malfunctioning e-pollbooks. It wasn't until last month that the Department of Homeland Security announced it would finally perform a forensic examination of the Durham County machines. That is not good enough. It is critical to secure our political parties, our campaigns, and the votes of Americans.

In 2015 and 2016, Russia hacked two Democratic campaign committees. Russian hackers also stole emails from John Podesta, Secretary Clinton's campaign manager. The Russian Government then leaked Democratic emails to influence the Presidential and, reportedly, House races in six States.

As I have emphasized at every part of my investigation, every part of my efforts, this is not a problem reserved for one political party. The National Republican Party committees have also all been hacked in the past, as well as the campaigns of Senator GRAHAM and our late colleague John McCain.

Political campaigns don't have the expertise or resources to protect themselves from foreign government hackers. They ought to be in a position to get assistance, and if Congress doesn't act, they are going to get hacked again in 2020.

That is why I introduced legislation earlier this year, the Federal Campaign Cybersecurity Assistance Act, to secure campaigns and State parties. This would apply to both Democrats and Republicans. The bill turns the party committees, like the Democratic National Committee and the Republican National Committee, into an ''IT department'' for their campaigns, State parties, and candidates. The parties will be able to give campaigns professionally managed, secured laptops, cell phones, and emails, which are much harder to hack. I think it is in the interest of our country, voters, Democrats, and Republicans to pass that bill.

I am going to close my remarks where I began, this extraordinary information that was compiled by the Associated Press that demonstrates that out-of-date software is going to be