Thank you, Mr. Chair and members of the committee. I am Max Hailperin, Professor Emeritus of Computer Science. Since 2010, my professional focus has been on computer systems used for election administration, and for that reason I served on the interim working group that Secretary of State Simon assembled to advise how Minnesota's election systems should be secured.

Because my perspective comes from the working group, I won't comment on the reporting and matching-fund provisions that are unique to the Senate's version of the bill. Instead, I'll address the question whether to appropriate a smaller amount of money focused specifically on the Statewide Voter Registration System (SVRS) or a larger amount of money with a broader focus.

From what I heard in the committee hearings and floor sessions, one reason some legislators think most of the funding can wait is because of how we've talked about our past experience. Secretary Simon has repeated countless times that Minnesota was one of 21 states targeted in 2016. And nearly as many times, this remark has been met with skepticism about just how serious the probing of our system was. Here's the truth: it doesn't matter. If Minnesota had been one of the other 29 states that didn't happen to be targeted at all, we'd still need to upgrade our election security. And it would still be an urgent matter. Our election systems had serious security needs even before 2016, and the only thing that has changed since then is that we're now several more years behind.

Another distraction has been the half of our glass that is full. We use paper ballots, and we use human eyeballs to check the tabulation of those ballots. That's great. But it does nothing to address the weaknesses elsewhere in the election process. In particular, a successful attack on SVRS or electronic pollbook systems could prevent voters from ever getting their paper ballots in the first place.

Before diving into the nuts and bolts of the working group's recommendations, I'll remark that the House language would not limit the Secretary to these recommendations, but would provide him flexibility to pay for other improvements that prove necessary. That flexibility has provoked some consternation, but as software developers like to say, it's not a bug, it's a feature. Let me illustrate why with a brief anecdote.

In January, after the working group wrapped up its work, the Department of Homeland Security issued an urgent alert, not specific to election systems. A new surge of sophisticated attacks against a very core part of the internet—the Domain Name System—made it imperative for all government agencies to immediately put certain mitigation measures in place, which the DHS listed. Those measures weren't expensive, but they were important. If another alert like that were to come out in the next few years, I'm quite sure you'd want the Secretary to respond immediately without another trip to the legislature.

The working group spelled out 20 specific action items. There is no surer way to make eyes glaze over than to step one-by-one through 20 bullet points, so instead I'm going to tie many of them together into a coherent package. I'm only going to directly touch on 10 of the 20 items, but they include the most expensive ones, such that they add up to $4.9 million, based on the estimates from the Secretary's office. Afterward I'll be open to questions, and you certainly are welcome to ask the question what the other 10 items are and why they too are important.

The Statewide Voter Registration System would be any attacker's favorite target for two reasons. It has a lot of angles from which it can be attacked, and it provides a lot of opportunity for damage. So it needs to be carefully reworked, module by module, to eliminate vulnerabilities. After 15 years of accumulated modifications, all resting on technologies with dwindling support, the system has grown rather rickety.

But modernizing SVRS isn't enough to protect it from attack. To start with, every county has access to the system, and so do many cities. If an attacker were to take over a computer that any of those local election offices uses to connect to SVRS, they could use it to submit data retrieval and update requests. The central SVRS server would respond to these requests as though they had come from an authorized election official. So SVRS can only be as secure as the local election offices. The two largest items after the SVRS modernization both aim to help city and county election officials with the improvements needed at their level. One is for monetary grants to fund the local improvements, and the other is the provision of cybersecurity training and consulting services to the local officials. As you know, most counties cannot realistically hire specialists in election cybersecurity. By using a shared resource—what the jargonauts are calling a cybernavigator—they can nonetheless have access to the guidance they need.

Several other items likewise are intended to prevent intrusion into SVRS. Rather than go into them, I'd rather turn to what happens when prevention fails. Even the best prevention will have blind spots, and so security professionals emphasize that a comprehensive strategy needs to include detecting and responding to successful intrusion—just like physical spaces need burglar alarms and cameras, not only locks on the doors.

Our key recommendation with regard to detection is listed in some documents as automated behavioral analysis, in others as Database Activity Monitoring. The idea is this: even if each individual database access appears innocuous, if the overall pattern is unusual, that should be cause for alarm. For example, suppose a normally quiet, rural county suddenly submits thousands of changes of address. If that were to happen as a result of bogus Voter Registration Applications, the local county auditor would surely have noticed thousands all arriving at once. But if it happens as a result of a cyber intrusion, then we need Database Activity Monitoring to exercise the same vigilance.

The Database Activity Monitoring system can immediately respond so as to limit damage, for example by shutting off all access by a particular user whose access appears to have been co-opted. However, it would also send information about any detected anomaly to the Security Information and Event Management system, another of our recommendations. That system is responsible for keeping all security-relevant information in a single timestamped log so that an investigator can work backward from the point an intrusion is detected and figure out what else had already occurred. It also categorizes events and immediately alerts on-call personnel to anything serious.

Once the cybersecurity experts investigate a detected intrusion and determine the extent of the damage, they need to get the system back to proper operation. That requires the ability to roll back any changes the attacker may have made in the stored data and programs. Using the current system of nightly backups, that would take so long that any attack would effectively turn into a denial-of-service attack while the staff loaded in the old backups and accounted for the changes since the most recent backup. Therefore, our group recommended switching to the modern Continuous Data Protection approach, in which all data is backed up all the time and earlier versions are instantly available.

All of these software components need to be protected from subversion using modern antivirus software. And they all need hardware to run on. For example, the Continuous Data Protection system relies on having additional storage devices. And new servers and networking hardware are needed to support all the other enhancements.

I'm sorry to have taken so long with this recitation of security components, but I hope I've illustrated that they aren't just valuable as individual items, but as interlocking, mutually reinforcing parts of a comprehensive approach. That's why funding just one item would be a mistake. It would be like building a stool, but starting with only one leg.

Much as I would like to wrap up, I feel I should explain one of the items not connected to SVRS—one that has attracted some skepticism. That's the provision of accessibility. I've heard some legislators question what accessibility is doing in a security bill, so I need to respond. There's an unfortunate tradition of talking about accessibility and security as though they were two separate topics. Even our working group fell into that trap. But really election accessibility is just one particular aspect of election security.

Because Representative Lucero spoke in both the Senate committee and the House floor session, I know you've all heard him emphasize that the three main security objectives are confidentiality, integrity, and availability—CIA. Those three apply to votes every bit as much as to voter registrations. Your vote shouldn't be disclosed to anyone else and it should be protected from modification by anyone else. And nobody should be able to stop you from voting. If you believe in those three security objectives for voting, and if you believe they apply to every eligible voter including those with disabilities, then accessibility is not a separate topic.

Thank you. I would be glad to take any questions.