Good Morning – It's great to be here in Boston! (As an Alum of UVM and lifelong hockey fan - Go Bruins!)

When I was first elected as VT Sec of State in 2010, my agency relied on paper-driven processes. It was a simpler time in terms of cybersecurity, but we were much less efficient with our resources and less user-friendly to our customers.

Today, we have transformed the Sec of State's office to a digital environment – going from almost 0% on-line activity to ~98%.

I never thought cyber security would be as big a part of my role as it has become!

Now, I eat, sleep and breathe cybersecurity.

I dream about firewalls, vulnerability assessments, and pen testing.

It's the new normal we live in after the Aug 2016 conference call with then DHS Secy Jeh Johnson & all Secs of State alerting us that Russian cyber agents were suspected of attacking our election systems.

Elections aren't the only systems at risk either.

Gov't agencies, from federal, to state, to municipal town offices, are more & more frequently being targeted by cyber bad actors, with increasing levels of sophistication.

That's the bad news.

The good news is… Secs of State around the country ARE doing the work necessary to protect our election systems.

The good news is… what used to be just an IT problem is now a priority as these issues have moved from the server room to the board room.

After the Nov 2016 election, much of the focus of the 21 states attacked was directed towards the 1 state that was breached.

It's important to remind folks that 20 states defended, and defended well.

The day after the 2018 Nov 6th general election – I had several national news organizations call me to ask what happened?

My response - NO NEWS IS GOOD NEWS!

What's the moral of the story?

We were in decent shape in 2016 BUT in even better shape in 2018!

However, you know and I know that our battle is far from over.

The enemies of our democracy are evolving their tactics daily.

If what they tried yesterday didn't work, I can assure you they're trying a different way today.

And if that doesn't work, they'll try again tomorrow.

We must remain vigilant – cybersecurity is a race w/o a finish line.

Whether we're looking ahead to 2020 elections, or how we can continue to protect any of our public sector systems, we know there will always be challenges ahead.

As public sector officials, we have a responsibility to do everything we can to protect the private data of the people we serve.

In fact, my cybersecurity journey in VT didn't start with elections. Rather, back in 2013 I heard from a colleague that hackers had penetrated their state's corporations database.

I remember coming back to VT, and asking my IT Director what our posture looked like – he said he thought we were strong.

But that we could be even stronger so we underwent a thorough, independent vulnerability & risk assessment of all of our systems.

VT and my team were fortunate, that was 2013, and luckily it gave us a jumpstart well ahead of the 2016 elections.

As many of you may know, I also currently serve as President for the National Association of Secretaries of State, known as NASS.

Much has changed since 2016, so where are we today?

We have made tremendous strides since 2016.

State and federal partners, working alongside private sector security companies, have truly come together to work as a team protecting our elections systems.

As DHS Cybersecurity & Infrastructure Security Agency (CISA) Director Chris Krebs has said in testimony before Congress, "the 2018 midterms were the 'most secure' in modern U.S. history…"

I can't thank Director Krebs enough for the support he and his team has invested in our states.

State and local autonomy over elections is one of our greatest assets against cyberattacks.

Our decentralized, low-connectivity electoral process is inherently designed to withstand and deter such threats.

Furthermore, states have been doing the hard work with DHS and private sector companies to conduct:

- **cyber hygiene scans,**
- **risk and vulnerability assessments,**
- **penetration testing,**
- **cyber preparedness training,**
- **putting increased resiliencies into place, and**
- **developing contingency plans for the inevitable attacks/breaches,**

Remember, if it is a computer, it can be hacked.

Anyone who tells you otherwise is misinformed - this is why we need to prepare, monitor, and plan to mitigate.

Secretaries and their staff have been conducting outreach and training for their local (or county) election officials – sharing:

- **resources,**
- **cybersecurity training**
- **best practices, and**
- **we continue looking for better ways/methods to provide**

If you want to secure the machine, a great first step is to secure the human!

The federal designation of elections as critical infrastructure has opened up additional federal resources for states, including the creation of an Election Infrastructure Government Coordinating Council (known as EIS-GCC) - I am a member of the Ex Comm.

This has enabled federal, state & local officials to share resources with improved communications.

The EIS-GCC has 29 members, of which 24 are state/local election officials.

We are working to improve threat information sharing, communications protocols, update elections-sector specific plans, while developing add'l resources for state/local election officials.

We established the Sector Coordinating Council (SCC) for non-government, private sector entities to better communicate with election officials and the federal government.

In April 2018, an Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) was formed - all 50 states are members, along with over 1500 local jurisdictions.

States have been provided with DHS sponsored Albert sensors on their election-networks to monitor & detect anomalies in real-time.

This information can then be shared with Secs of State, their IT staff and election offices around the nation.

I tell you all this because it provides a brief snapshot into the vast amounts of work being done between federal, state, local, and private sector partners, and that work IS paying off.

For instance, in August 2018, my IT Director saw in our WAF logs, which we monitor routinely, an attempt to access our system which was blocked by our robust defense network.

What stood out about this attempt - our logs clearly stated "Russian Federation" as country of origin.

We notified our partners at DHS, CIS, & EI-ISAC and they were able to review and rapidly share that information with other states.

This focused, concerted effort helped increase situational awareness for all.

We did not have this capability before 2016.

We, as Secs of State, take the work of protecting our election integrity with incredible seriousness, and act rapidly when a situation presents itself.

I'm sure each and every one of you knows that there's still work to do, and challenges ahead.

Effective cybersecurity takes diligence & vigilance, and it isn't free.

Meeting the ongoing demands for updated equipment and ongoing cybersecurity upgrades requires funding that is too often limited.

In April 2018, Congress provided the remaining $380 million "hanging chad" dollars from the Help America Vote Act of 2002.

However, this did not and does not solve all the challenges we face.

We are thankful for this money because it helps our states enhance:

- **efficiency and security of elections,**
- **purchase of new voting systems,**
- **implementation of additional cybersecurity tools, and**
- **hiring of additional IT professionals.**

Now I'm going to speak solely as VT Sec of State, and not as NASS President.

We can't solve long-term, on-going challenges with lump sum monies every 15 years or so.

i.e. If you don't pay your electric bill - it gets shut off - a case of batteries may get you by for a while, but those batteries eventually run out.

In this case, when Congress provided the remaining $380 million from 2002 HAVA funds, it had been over 15 years since states had received an influx of election dollars.

Vote tabulators and software are no different than any other piece of equipment.

Raise your hand - if any of you still use a computer you bought 15 years ago.

I believe states need ongoing, sustainable funding from Congress, so we can keep innovating & evolving while doing the daily work necessary to defend our systems sustainably into the future.

We know the threat landscape - they tried once with few repercussions from the administration.

We know there will be attacks on our elections in 2020.

We need to build that wall - No, not the wall on the border – we need a wall protecting our democracy!

States need these critical resources NOW in 2019, not next year, to ensure we have the strongest cyber security posture going INTO next election season.

Remember – the 1st Presidential Primaries are in 7 months!

Congress needs to understand that buying new election equipment isn't like walking into Best Buy and saying "I'll take 200 of those."

Procurement takes time, every state has different rules/requirements.

My concern is that certain members of Congress are using election security as a partisan football, blocking meaningful progress.

It's time for the games to end – there is too much at stake and this is a serious business.

We need sustainable funding to allow states to plan/implement election security enhancements to counter emerging cybersecurity threats. It's time for Congress to heed that call.

So, outside of funding, what do our challenges look like?

Well, understand that in many instances, the true goal of foreign adversaries and cyber bad actors is not just to get in to our systems and do damage, but to:

- **sew chaos and discord through public perception, and**
- **weaken voter confidence in the integrity of our elections.**

Combatting misinformation/disinformation on social media is one of our greatest challenges looking forward.

In this day and age, it doesn't take long for disinformation posted by an orchestrated foreign entity to be shared and seen hundreds of thousands, and even millions, of times.

By the time that post is taken down, the damage has been done.

We are working hard with DHS, FBI and other intelligence agencies to educate our voters that state & local election officials are and should be the trusted sources for election information such as:

- **registering to vote,**
- **requesting an absentee ballot,**
- **polling locations and times, and**
- **actual voting.**

We're also working with social media companies like Facebook and Twitter to improve reporting channels.

There is still work to do - we all have a responsibility in this work, from companies providing the platform, to each of us individually.

We need to be careful what we share, look for trusted/verified sources, and treat social media disinformation/misinformation like a suspicious package at the airport: see something, say something!

Lastly, for any public officials listening, there is still work you can do to help secure our public sector systems.

Remember - new technology often comes with increased security.

Ensure that physical security goes hand in hand with cybersecurity.

For instance, physical storage and strict chain of custody for vote tabulators and memory cards is as important as the cyber defenses in place around our voter registration system.

Utilize best practices like using different trusted vendors from year to year for your penetration testing, to get a different set of eyes on your system.

Better protect your systems with multi-factor authentication, developing redundancies like daily backups AND build cybersecurity requirements into the procurement/RFP process from the get-go.

Plan for the worst – hope for the best - recognizing that at some point your system WILL be compromised, and take the steps necessary to reduce the amount of damage if the bad guys get in!

Lastly, invest in training for anyone with access to your systems.

Approx. 80% of all breaches originate with a phishing email.

One wrong click can do a world of damage - THAT is the reality of the digital world we live in today.

I'll close by saying - as election officials, we are doing the hard work necessary to protect our elections, but we can't take a day off!

Defending our Democracy is hard work… but worth every penny!

With that, I'm happy to open it up for questions!