Cybersecurity Task Force Meeting One DRAFT MINUTES, April 17, 2018

Part One

Secretary Merrill:

- Elections are safe from cyberattack
- Thanked all those here who protect CT and its cybersecurity
- 2018 will be the most difficult election year so far, as many will be focused on how secure those elections will be
- Merrill was informed a year later about the fact that CT was one of the 21 states targeted by Russian hackers
- Our elections are secure, and they are decentralized, making them safer - this was more an attack on our faith in the electoral process and system
- Revealed the budget for our increasing of cybersecurity - the money comes from remaining accounts for HAVA (Help America Vote Act).
- Reviewed the enormous number of voter registrations in CT these past years
- Recognised that this is a public meeting and therefore some questions cannot be answered as some require clearance to access that information.
- Introductions around the room

Part Two

Deputy Secretary Bates, following Merrill's introduction:

- What has 2016 done to illuminate possible vulnerabilities of our state's cybersecurity?
- Today it is the Russians, but tomorrow it could be another hacking group
- Russian motivations - reviewed Russian transgressions such as Estonia being denied internet services by Russian hackers a decade ago, and Russia's tampering with Ukraine's emerging democracy in 2014.
- Putin sees US promotion of democracy as a threat to Russian security, therefore elections and democracy must be delegitimised.
- Recounted recent US history with cybersecurity
- Hackers' aim is to undermine public faith in US elections
- Stressed the importance of information sharing and praised the gathering

Secretary Merrill:

- Described the various technologies we could employ/might currently be using
- States guard their cybersecurity abilities jealously from others
- Importance of identifying the nature of the threat and the communication structure reporting and sharing this information
- Possible area of focus for the task force: state level to the local level, as this is potentially the weakest area
- Nationally, the communications apparatus is pretty solid. Local level is more cause for concern.
- Mentioned the debate amongst the Secretaries of State in the state vs federal role in cybersecurity maintenance.

- We have a 20 year old closed loop system that varies by towns, but is kept off of the internet
- Noted there are no counties in CT so we have loads of towns and cities with various challenges and strategies

Mark Raymond:

- Outlined the equipment capabilities of the statewide network. He manages and secures the connections to the municipalities

Deputy Secretary Bates on behalf of Arthur House:

- We cannot shift from the digital age, and offense is inherently stronger than defense. States have a vital role in this struggle.

Part Three:

Commissioner Schriro:

- State police are responsible for the security of some of the towns
- Mentioned an FBI task force for cybersecurity improvement
- Remarked on the necessity of training: State police, POST local police, and fire service gets trained in cybersecurity, and this could be used by local election officials to train
- State statutes regarding voting security should be up for review.
- FBI has changed its reporting structure, 'cyberspace.' On the lookout and better reporting of cybercrimes - FBI is playing catchup as well.

Secretary Merrill:

- Remarked on Schriro's point of examining the statutes, was very receptive to the brand new idea

Tom Miano:

- Online and central voter systems are led by BEST
- Enhance CVRS system, and mentioned the two-factor authentication system

David Geick from BEST:

- RVA: vulnerability assessment by Homeland Security, scans all relevant systems for tampering

Tom Miano:

- Contingency voter lookup system in the cloud independent of the state's network (for election day registrations)
- DHS housing scans for the cloud's security, should eventually happen as of the last DHS meeting

Mark Raymond:

- State Cybersecurity strategy has seven points
- Cybersecurity draft plan is almost complete
- Incident Response Plan how the state might react to small/medium issues, use for businesses and private entities too
- Disruption Response Plan (NIMS model) for large issues
- Training executive staff of government officials
- Monthly discussions for cybersecurity held by Governor, Schriro, and Raymond

Peggy Reeves:

- CT is highly decentralised like most New England states\
- This is a strength but also has weaknesses in that such a decentralised system as many access points for things to go wrong

Homeland Security:

- Mentioned a catalog of resources
- Prioritize voting security issues
- Merrill asked about other states in NE creating task forces, he said he only knew of Vermont's cybersecurity advisory meetings (most similar to us)

Tom Miano:

- Responding to Laura Devlin: CVRS connects the town through special routers
- Vulnerability thereof: the work stations where the routers are not secure enough, someone can go there and tap into the system.

James Krupienski:

- Talked about how in his town they have a two-fold system, where he can balance one system in use to a backed up database. He heralded the use of the paper system

Part Four

Peggy Reeves:

- Reviewed the budget. Not enough to update the machines, but enough to improve security. Money must be used by 2023.

Sen. McLachlan:

- Biggest loophole is the voter roles
- The communications link (between town halls and the SOTS) is strong and secure. This is very important and the firewall could be hardened.

Secretary Merrill:

- No state's systems are currently run through the internet, all run on closed systems. Very happy with the scanning and voter tally machines

Mark Raymond:

- Can some of the budget be used in targeted repairs/replacements of these voting machines?

Alex Schwarzmann:

- Voting machines were installed in 2006, currently no worries about the hardware. Simple machines that are easily repaired. Newer doesn't necessarily mean better.

Secretary Merrill:

- Maintenance contracts are handled at the local level

Rep. Devlin:

- Mentioned LHS and the voter center in a question posed to Schwarzmann

Schwarzmann:

- LHS programs a few memory cards, and some are randomly selected for audits. All are checked by the voter centre to ensure they weren't tampered with before the election and are all programmed correctly.
- Voter Center guarantees the integrity of the memory cards as a safeguard

Part Five

Secretary Merrill:

- CT is in a good place
- We need to increase non-arduous auditing
- Maintaining the public's faith is the most important task.

Next Meeting is May 17, 2018.