October 23, 2020

Dear Colleagues,

As someone who served for 28 years as the Leon County Supervisor of Elections, I understand the weight of the responsibilities you carry. This election is particularly difficult with the pandemic, lack of poll workers, high voter turnout, political divisiveness, and concerns about the ever-increasing risks of attempted cyberattacks on our election systems, which have already begun.

One thing I think you all share is a desire to do the right thing. That is why I am compelled to warn you of a danger that I don't believe has been fully explained to you by the Division of Elections, and to offer you some solutions.

Specifically, the wireless modems that some of you are planning to use to transmit election results utilize Verizon, Sprint, or other 4G technology. These modems are as hackable as any cell phone. Encryption of the USB flash drives and a digital signature offer limited or no protection against a nation-state cyberattack.

The National Institute of Standards and Technology (NIST) and top computer security experts have warned that these modems can be hacked remotely. The Center for Internet Security said, "When networked devices are connected to the voting system, this connectivity provides an access path… through the internet, and thus an attack can be orchestrated from anywhere in the world."[1]

NIST warns that using cellular modems, or connecting a county's central tabulator to WiFi (the internet) can allow remote hackers to gain access to an entire voting system, inject malware, change election results, or create chaos through denial of service attacks. Firewalls do not offer complete protection. They can be breached.

[1] Center for Internet Security, A Handbook for Elections Infrastructure Security, Introduction, Page 11, https://www.cisecurity.org/elections-resources

Some of you may have the mistaken belief that Florida's wireless modems have been federally certified by the Election Assistance Commission (EAC), but they have not. Furthermore, the Elections Assistance Commission (EAC) reprimanded[2] Election Systems & Software (ES&S) for falsely stating that the wireless modems had received federal certification when that is not the case. The EAC required ES&S to send a letter[3] to each of its customers to inform them that the modems are NOT federally certified. You should have received this letter from ES&S but if you did not, you can read it by clicking on the link in footnote 3 below.

As you know, Florida does not require federal certification of its voting systems. The Florida Bureau of Voting Systems Certification relies on the 15-year-old Voting Systems Standards.[4] It is astounding that with all the cyber advice that has supposedly been given to Florida election officials, this critical vulnerability has been allowed to remain uncorrected.

In order to receive wireless modem transmissions on Election Night, your central tabulator must be connected to the internet to receive the transmissions. The only thing that protects your central tabulator from a cyber attack is the firewall. Many Florida counties have a Cisco firewall, which in May 2020 published information about a gaping security vulnerability in its firewalls. [5]

There are many several alternative ways you can communicate vote information without needlessly exposing your system to online attacks:

1) Results can be reported orally by phone.
2) A picture of the poll tapes can be texted or emailed to the elections office.
3) Removable media (such as memory cards and USB flash drives) from the scanners or voting machines can be physically transported to voting headquarters at the same time as the ballots and poll tapes, which must be transported anyway.

---

[2] Reprimand letter from EAC to ES&S https://freespeechforpeople.org/wp-content/uploads/2020/08/letter-to-hostetler-and-greenhalgh-8.7.20.pdf
[3] ES&S letter required by EAC to be sent to all ES&S customers with wireless modems: https://freespeechforpeople.org/wp-content/uploads/2020/08/letter-to-hostetler-and-greenhalgh-8.7.20.pdf
[4] Florida Voting System Standards, January, 2005, https://dos.myflorida.com/media/693718/dsde101.pdf
[5] Vulnerabilities and fixes, Cisco firewalls, https://www.darkreading.com/perimeter/cisco-fixes-vulnerabilities-in-asa-firewall-found-by-positive-technologies/d/d-id/1337778

4) Data can be transmitted using internet technology, so long as that technology is air-gapped, meaning that it is kept completely separate from the tabulation system and election management system at both ends.

You can transmit data in two different ways – one that is quick (1 or 2 above) and one that is the most secure (3 or 4 above). Duplicate systems offer an added layer of protection.

Please check with your IT department or with the Department of Homeland Security to be sure you have followed the recommendations to update, patch, and protect your firewall. Please also make sure that you have the most recent security updates for your Windows 7 or other operating system.[6]

Again, the ideal solution is to remove your central tabulator from the internet completely and to not use your wireless modems.

I debated whether to send you this letter since it is so close to Election Day, but I believe that warning or reminding you to secure these vulnerabilities is the wisest thing to do. Our nation's enemies are certainly already aware that they exist and attempts to compromise this election have already begun.[7]

I wish you all a safe and successful election.

Respectfully,

Ion Sancho

[6] Windows 7 security updates https://www.zdnet.com/article/windows-7-end-of-life-security-risks-and-what-you-should-do-next/
[7] NY Times, Election Threats, https://www.nytimes.com/2020/10/22/us/politics/russia-election-interference-hacks.html