SMARTelections.us

August 2, 2023

New York State Board of Election Commissioners

Douglas A. Kellner, Co-Chair
Peter S. Kosinski, Co-Chair
Anthony J. Casale, Commissioner
Andrew J. Spano, Commissioner

Dear Election Commissioners,

Apologies for sending these notes so soon before your meeting.

ES&S NOT SECURE, NOT TRUSTWORTHY

ES&S DANGEROUSLY DOWNPLAYS SECURITY RISKS

In recent comments to a blog post ES&S downplayed the potential risk to New York elections via a software attack. They called Professor Appel's concern a "highly improbable attack scenario" saying it was "an extreme hack" that was "incredibly complicated, if not nearly impossible."

Such an "extreme hack" has already taken place. It's called Solar Winds.

- **"Researchers believed at least 1,000 very skilled, very capable engineers worked on the SolarWinds hack. This is the largest and most sophisticated sort of operation that we have seen"**
- Solar Winds penetrated the security of "companies including Intel, Nvidia, Cisco, Belkin, and VMWare ... as well as the US Treasury, Commerce, State, Energy, and Homeland Security departments."
- Here is a Solar Winds timeline.
    - "the attacks are largely thought to "**have begun as far back as October 2019**…when hackers breached the Texas company SolarWinds."

    - **Solar Winds was not detected until December 2020.**
    - On November 12, 2020 when CISA said, "The November 3rd election was the most secure in American history.". Hackers had likely already been inside CISA's parent agency DHS for months.
- Media reports said the "hack was so sophisticated that it would have been pretty hard for anybody to fight it" and described it as, "a sprawling, monthslong cyberespionage effort."

ES&S WAS ALREADY COMPROMISED

In August of 2017 a security researcher at Upguard discovered a database overseen by ES&S that was incorrectly configured to be completely public. **The database "included encrypted versions of passwords for ES&S employee accounts."**

"The worse-case scenario is that they could be completely infiltrated right now," said Upguard's director of strategy Jon Hendren."

The balance of power in the U.S. House of Representatives will likely be determined in New York in 2024. That might be something that would bring out sophisticated hackers. We must be extremely careful not to give them an opening. **If our system is hacked via known vulnerabilities that have been pointed out to the New York State Board of Elections for years, people will understandably hold you responsible.**

ES&S HAS REPEATEDLY LIED TO THE NYS BOE

In their application in 2019, ES&S lied multiple times regarding litigation that they were legally required to reveal to the NYS BOE.

In their new application, ES&S also hid litigation.

> **From:** Douglas A Kellner <dak@khgflaw.com>
> **Date:** July 28, 2023 at 12:38:07 AM GMT+1
> **Subject: ... Another ES&S Express Vote Bar Code Lawsuit: Arkansas Voter Integrity Initiative v. Thurston**

> … "ES&S did not disclose the Arkansas litigation in their certification application pending in New York, although they were required to do so. 9 NYCRR § 6209.4(i)"

ES&S also distributed information to the New York legislature, the public and the media that security experts called "irresponsible and misleading" and "disingenuous."

THERE MUST BE ACCOUNTABILITY

A vendor to the state cannot repeatedly lie to the NYS BOE, the public, the media and the New York legislature with impunity.

ES&S lack of regard for the truth also makes their statements downplaying security risks less believable. If there were risks, would they acknowledge them? No they would not.

As we said in previous communications:
The ExpressVote XL does not meet New York Statutes.

As we further demonstrated in this letter
The ExpressVote XL is not safe, and ES&S cannot be trusted in their claims that it is safe.

Please reject it for use in New York State.

Thank you.

Kind Regards,
Lulu Friesdat
Co-Founder & Executive Director, SMART Elections