August 26, 2019

The Honorable Roy Blunt
Chair, Senate Committee on Rules & Administration
United States Senate
Washington, DC 20510

The Honorable Amy Klobuchar
Ranking Member, Senate Committee on Rules & Administration
United States Senate
Washington, DC 20510

The Honorable Zoe Lofgren
Chair, Committee on House Administration
United States House of Representatives
Washington, DC 20515

The Honorable Rodney Davis
Ranking Member, Committee on House Administration
United States House of Representatives
Washington, DC 20515

Dear Chair Blunt, Ranking Member Klobuchar, Chair Lofgren and Ranking Member Davis,

We thank you for your leadership on the Senate Committee on Rules & Administration and the Committee on House Administration and commend your work to refocus the committees on the critical national security threat facing our election systems. The findings in the recently released report from the Senate Select Committee on Intelligence (SSCI) reaffirmed a grim reality that we already knew: our elections are under attack and our voting systems are insufficiently secure to resist a committed, advanced and persistent attacker. As part of your investigation into this threat, we urge that your committees conduct a hearing on election security. The ideal panel for such hearings will include testimony by election security experts and representatives of the major voting system vendors. As explained below, vendor testimony is critical to understanding the threats, but the experience of the Senate Rules Committee teaches that, if simply invited to testify voluntarily, the vendors may not show.

The security of our nation's elections is acutely dependent on the vendors that supply our computerized voting systems. Recent news reports have disclosed troubling weaknesses in commercially marketed voting systems and disturbing conduct by voting system vendors, raising significant questions that are unanswered. The voting system vendors have operated with little oversight and no regulation for decades. Given the gravity and urgency of this issue, we write to you to urge the committees to hold a

hearing on election system security featuring sworn testimony from officers of the voting system vendors to shed more light on their practices which directly impact the security of the nation.

On July 13, 2019, the *Associated Press* published a report revealing that all of the newest federally certified voting systems from the largest voting system manufacturer, Election Systems & Software (ES&S), rely on aged Windows 7 operating systems which will soon be "end-of-life" in January 2020.[1] The *AP* also reported that systems sold by Hart Intercivic, the third largest vendor, used Windows 7 embedded which will "end-of-life" in October 2020. This means that the election systems ES&S and Hart are selling to local election officials *today* will be using outdated software in just a few short months, about the same time customers take delivery on their "new" election systems in the midst of the 2020 election cycle. The security implications of this disclosure are troubling enough, but this news also raises important questions about these vendors' sales and marketing practices. The events suggest that these vendors were actively and knowingly selling systems that rely on soon-to-be outdated software.

This is not the only deeply disquieting report regarding the security practices and sales conduct of the voting system vendors. In February of 2018, *The New York Times Magazine* reported that ES&S pre-installed remote-access software on its election systems, or recommended that election administrators install remote-access software on ES&S systems.[2] ES&S issued a categorical denial to the *Times*, asserting that it never installed remote-access software on its systems.[3] However, in response to a letter from Senator Ron Wyden (OR), ES&S reversed itself and admitted that it did in fact, install remote-access software on some of its products.[4] The inclusion of remote-access software in voting equipment introduces profound security risks and raises serious questions about the security profile of ES&S systems. Moreover, ES&S's initial untrue denial to the *Times* raises separate concerns regarding the firm's integrity.

Last summer, it was reported by *McClatchy* that ES&S has established a previously undisclosed board of advisors comprised of election officials responsible for negotiating sales and service contracts.[5] The report revealed that these officials are regularly treated to travel to locations including Las Vegas, New York City and Florida, creating at a minimum, the appearance of a conflict of interest. Hart Intercivic responded to reporters' questions and confirmed that it does not have a similar board, but Dominion Voting refused to answer reporters' questions, leaving open the possibility that it maintains a similar structure.

The North Carolina State Board of Elections recently sought information from the three top voting system vendors, Dominion Voting, ES&S and Hart Intercivic, regarding their ownership. All three vendors gave incomplete information regarding their financial backers, leaving many open questions.[6] After it was revealed that a Russian oligarch had a major ownership stake in the company that maintains Maryland's voting systems, changes were made. Transparency about who owns and funds our voting machine vendors is critical. In today's threat environment it is essential not only to know who owns the companies that develop and program the proprietary, non-public software that counts our votes, but also

---

[1] Tami Abdollah, "AP Exclusive: New election systems use vulnerable software," *Associated Press,* July 13, 2019
[2] Kim Zetter, "The Myth of the Hacker-Proof Voting Machine," *The New York Times Magazine,"* February 21, 2019
[3] Ibid.
[4] Kim Zetter, "Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems It Sold to States," *Motherboard,* July 17, 2018
[5] Greg Gordon, Amy Renee Leiker, Jamie Self, Stanley Dunlap, "Voting machine vendor treated election officials to trips to Vegas, elsewhere," *McClatchy,* June 21, 2018
[6] Emery Dalesio, "Who's behind voting machine makers? Money of unclear origins," *Associated Press,* July 12, 2019

to know where these systems are engineered. In 2016, it was reported that Dominion Voting Solutions develops its software outside the U.S. in Serbia.[7]

Furthermore, many states and localities contract with smaller companies to service, maintain and program their voting equipment. This creates another potential vulnerability in the voting system supply chain that has been mostly ignored by election administrators and the U.S. Election Assistance Commission.[8] The role these third-party vendors play and the potential risks they introduce demand further scrutiny.

The above represents just a fraction of issues relevant to the voting system vendors that we believe beg close examination. We note that last year the Senate Rules Committee attempted to hold a hearing with testimony from representatives of the election system industry, but only one of the top three vendors chose to show up. Therefore, we think it imperative for the Committees in both Houses to require participation by the voting system vendors in a hearing on election security.

We stand ready to assist the committee staff in any way necessary. We thank you for your consideration and for your commitment to securing our cherished democratic process.

Sincerely,

National Election Defense Coalition
Davis, California

Public Citizen
Washington, DC

R Street Institute
Washington, DC

Project on Government Oversight
Washington, DC

National Association for the Advancement of Colored People
Washington, DC

OSET Institute Inc.
Palo Alto, California

League of Women Voters
Washington, DC

FreedomWorks
Washington, DC

Free Speech for People
Amherst, Massachusetts

Common Cause
Washington, DC

Electronic Privacy Information Center
Washington, DC

Daily Kos
Oakland, CA

Protect Democracy
Washington, DC

[7] Patrick Thibodeau, "One election-system vendor uses developers in Serbia," *Computerworld,* October 5, 2016
[8] Kim Zetter, "Experts: Elections commission downplaying unseen risks to 2020 vote," *Politico,* March 13, 2019