SMARTelections.us

November 21, 2019

A letter from a member of our Technical Advisory Team:
Chris Vickery | Director of Risk Research; Upguard

The current hardware and software that form the US elections infrastructure are fraught with vulnerabilities which, unless confronted, will continue degrading public trust in the integrity of our elections.

In the course of my research since 2015, I have come across nationwide, US voter databases exposed to the global public Internet on at least four separate occasions. Lax policies and laws allowing those concentrated masses of Personally Identifiable Information cannot persist if we wish to have free and fair elections. It is far too easy for nefarious entities to weaponize those types of intense collections for the purposes of not only altering registration details, but also other acts which further impede the voting process.

Despite what manufacturers claim, ballot casting and ballot counting devices are far too loose in accepting arbitrary input. Researchers routinely demonstrate the utter lack of security exhibited by even the most up-to-date elections machinery. Electronic poll books as well as the laptops which manage elections sites open even more vectors of potential attack. All these devices feed data upstream to aggregate points of collection, tabulation, and reporting. ***Any one of them represents an insertion point at which malicious actors can have an unexpectedly wide effect on the entire chain of system interactions.***

In the past, it has often been believed that criticism and technical scrutiny of the devices and processes involved in casting and counting ballots causes undue fear and doubt in the fairness of the results. This mindset is untenable and cannot be allowed to persist. Stifling legitimate concerns is never the answer and ultimately serves the interests of bad actors who seek to exploit the vulnerabilities, which give rise to those same legitimate concerns.

Reform is needed. I support SMART Elections efforts to direct resources to states, tied to strong security requirements in order to ensure they actually improve our election security.

Chris Vickery

Please note:
Affiliation is for identification purposes only and does not signify organizational endorsement.

Chris Vickery has been cited as a cyber security expert by The New York Times, Forbes, Reuters, BBC, LA Times, Washington Post, and many other publications. In the course of his work he has assisted the MPAA, Thomson Reuters, Microsoft, Citrix, AARP, Verizon and dozens of other entities in plugging serious data breaches affecting hundreds of millions of individuals. He has assisted investigations conducted by entities such as the FTC, FBI, Texas Attorney General's Office, Secret Service, HHS, and the State of Kansas.