A Law is Expiring That Allows Ethical Hackers to Help Protect U.S. Elections

- By Joseph Marks Senior Correspondent, Nextgov Read bio ▸

October 11, 2017

Topics

- Cyber
- Elections

John Minchillo/AP

AA Font size + Print

Early voters use electronic ballot casting machines at the Franklin County Board of Elections, Monday, Nov. 7, 2016, in Columbus, Ohio.

- F≡cebook
- Twi??e!
- LinkedIn
- ▸ m≡il ?his ≡!?icle

- By Joseph Marks Senior Correspondent, Nextgov Read bio ▸

October 11, 2017

Renewing a Digital Millennium Copyright Act exemption for ethical hacking is vital for election security, researchers say.

A division of the Library of Congress could play a key role in ensuring future U.S. elections are protected against cyberattacks that alter vote tallies or other digital meddling, the authors of a major report on election hacking said Tuesday.

That division, the U.S. Copyright Office, approved a slate of exemptions to a 1996 copyright law last year that give ethical hackers more leeway to search for digital vulnerabilities in products without facing legal threats from companies that don’t want their security gaps exposed.

The exemption, which came out shortly after the 2016 election, included a specific provision freeing ethical hackers to poke and prod at voting machines.

That provision paved the way for a “voting machine hacking village” at the 2017 DEF CON security conference in Las Vegas in July that turned up cyber vulnerabilities in numerous voting systems.

If the exemption is allowed to expire in 2018, however, it could leave future elections more vulnerable to nation-state and criminal hackers, DEF CON organizer Jeff Moss said during an event releasing a report on the hacking village’s findings Tuesday.

DEF CON hackers found that numerous voting machines were highly vulnerable to digital attacks when the hacker had in-person access to the machine, according to the report.

One decommissioned device at the challenge could also be hacked remotely over a Wi-Fi network.

The hackers also found evidence of an expansive supply chain for voting-machine components that wound through China and numerous other nations, according to the report. That supply chain provides numerous opportunities for nation-states and criminal groups to insert corrupted computer chips or other components that could later process vote-altering malware, panelists said during the report release event at the Atlantic Council think tank.

Another major risk factor, according to panelists, is consolidation in the voting machine industry, which has dropped the number of major suppliers from 20-something to about four over the past decade.

That means attackers hoping to compromise U.S. elections have a much smaller attack space to target than they did several years ago, former National Security Agency official Sherri Ramsay said.

It also contradicts a common claim by state and local election officials—that voting systems vary so much district by district that a single hacking group would never have the resources to compromise a large number of them, Jake Braun, a former Homeland Security Department official, said.

“We now know that’s false,” Braun said. “Through a handful of simple attacks on manufacturers not in the U.S., Russians could implant malware onto thousands of machines at once without ever leaving the Kremlin.”

Russian government-linked hackers probed election systems in about 21 states during the 2016 election, the Homeland Security Department and intelligence community concluded, but there’s no evidence they penetrated those systems or changed any vote totals.

During next year’s DEF CON, Moss said, he hopes to work with voting-machine manufacturers and state and local election officials so that hackers can test both the voting machines themselves and the backend systems that tabulate votes and share vote totals between districts.

Voting-machine companies have not responded to Moss’ requests yet, he said. He’s hopeful, however, that a renewal of the Digital Millennium Copyright Act exemptions that enabled the hacking competition will spur some of those companies to cooperate.

Security researchers are pressing the Copyright Office to expand that provision to give ethical hackers more legal protections and make it easier for them to share information about their discoveries and concerns.

One issue, Moss said, is that DEF CON hackers were barred from publishing software code from the voting machines or sharing the code with researchers who weren’t at the event. That makes it more difficult for researchers who can’t get ahold of their own voting machines to vet the DEF CON findings or to search for additional vulnerabilities.

DEF CON organizers purchased voting machines for the hacking village primarily on eBay where they’re infrequently available.

Also during Tuesday’s event, the Center for Internet Security announced it will develop a best practices handbook for securing election infrastructure. The center manages a cybersecurity information sharing program for state and local governments.

- Joseph Marks covers cybersecurity for Nextgov. He previously covered cybersecurity for Politico, intellectual property for Bloomberg BNA and federal litigation for Law360. He covered government technology for Nextgov during an earlier stint at the publication and began his career at Midwestern ... Full bio ▸

- F≡cebook
- Twi?⃝?⃝e!⃝
- LinkedIn
- ▸ m≡il ?⃝his ≡!⃝?⃝icle

✉ Enter your email to get c Subscribe

Most Read

1. 1
   How the US Army is Preparing to Fight Hybrid War in 2030
2. 2
   ‘I Want to Finish This’: US Special Ops Leaders Urge Washington to Stick by the Syrian Kurds