POLITICO

MORNING CYBERSECURITY

November 6, 2019

BY **TIM STARKS**

With help from Mary Lee, Martin Matishak and Matthew Brown

Editor's Note: This edition of Morning Cybersecurity is published weekdays at 10 a.m. POLITICO Pro Cybersecurity subscribers hold exclusive early access to the newsletter each morning at 6 a.m. Learn more about POLITICO Pro's comprehensive policy intelligence coverage, policy tools and services at www.politicopro.com.

QUICK FIX

— **Some of the people who need the most cybersecurity help are getting some,** with DHS rolling out a guide on how small businesses and state and local governments can enhance their safeguards.

— **The lack of skilled cybersecurity workers is getting worse, not better,** an organization of cyber pros found.

— The lack of skilled cybersecurity workers is getting worse, not better, an organization of cyber pros found.

— With little time to spare, the Senate Judiciary Committee will hear from national security officials today about re-upping expiring surveillance provisions.

HAPPY WEDNESDAY and welcome to Morning Cybersecurity! Oh, cool, that totally makes sense. Let's just get off your lawn, then, non-franchise filmmaker. Send your thoughts, feedback and especially tips to tstarks@politico.com. Be sure to follow @POLITICOPro and @MorningCybersec. Full team info below.

CYBER DRILL — Riots, scandalous deep fakes and martial law: Those were just a few situations for law enforcement officials and experts to contend with during Cybereason's "Operation Blackout" simulation on Tuesday. The exercise, hosted at the Washington, D.C., law firm Venable, simulated worst-case scenarios from catastrophic cyberattacks on the 2020 presidential election. Participants included officials from the Secret Service, DOJ, DHS, FBI, as well as local and state law enforcement.

In this simulation, a red team deployed attacks — such as disinformation campaigns and phishing attacks — against a defending blue team tasked with beating back the hackers. In the end, neither team prevailed, but it did showcase how hackers could disrupt an election without ever attacking a voting machine or election technology. In fact, the rules of the game made attacks on voting equipment off limits, so "we wanted to bridge the cyber to physical gap quickly," said Yonatan Striem-Amit, Cybereason's co-founder and red team leader. That essentially meant taking down the city instead.

TWEET OF THE DAY — It seems so long ago.