Issued 7/23/18

States Slow to Prepare for Hacking Threats

U.S. intelligence officials and security experts have spent years urging states to shore up their elections' digital defenses, and the latest indictments from special counsel Robert Mueller drew fresh attention to Russia's cyberattacks on the 2016 presidential election. But less than four months before the midterm elections, most states' election offices have failed to fix their most glaring security weaknesses, according to a POLITICO survey of all 50 states. And few states are planning steps that would improve their safeguards before November, even after they receive their shares of the $380 million in election security funding that Congress approved in March. Only 13 states said they intend to use the federal dollars to buy new voting machines. At least 22 said they have no plans to replace their machines before the election — including all five states that rely solely on paperless electronic voting devices, which cybersecurity experts consider a top vulnerability. In addition, almost no states conduct robust, statistic-based post-election audits to look for evidence of tampering after the fact. And fewer than one-third of states and territories have requested a key type of security review from the Department of Homeland Security. States have to take the threat seriously and not just wait for federal help, said Sen. James Lankford (R-Okla.), a member of the Intelligence Committee and one of the chief sponsors of the Secure Elections Act, a bipartisan bill meant to bolster security at the polls. "It is not the federal government's responsibility to pay for new machines for you; do what is your state's responsibility to be able to take care of your own elections and make sure they're secure." Lankford said he does not think states are being "apathetic" about implementing security safeguards at the polls. "Russia tried

to meddle in our 2016 elections — they'll be back in 2018 and 2020," Lankford tweeted Tuesday. On Capitol Hill, both the Senate and House intelligence committees have weighed in on the election hacking issue in their separate Russia investigations, with both panels recommending that voting machines use paper ballots. The five states that rely entirely on paperless voting machines are Delaware, Georgia, Louisiana, New Jersey, and South Carolina. In Georgia, lawmakers failed in March to pass a bill to replace the state's electronic machines by 2024. As in South Carolina, election integrity groups are suing the state over voting security issues. Some states said they simply didn't receive enough money from the federal government to make much of a change in their systems. Indiana, Kansas, Nebraska and Texas told POLITICO the amount of federal funding was not enough to overhaul their vast, statewide election systems. So far, there's been no indication hackers have tampered with voting machines or other systems in ways that have changed the outcome of an election. However, the Department of Homeland Security believes that Russians "scanned" all 50 states potentially looking for vulnerabilities in voter registration databases, senior DHS official Christopher Krebs said recently. Voter databases are among the most vulnerable elements of the U.S. election system because they are connected to the internet and are often maintained by inadequately staffed or poorly trained IT departments. States have been slow to take advantage of additional federal assistance for elections. DHS offers states help in securing election technology, which the department in early 2017 designated "critical infrastructure" on par with hospitals and power plants. But the department has received requests from only 18 states and territories for risk and vulnerability assessments, Matthew Masterson, a senior cybersecurity adviser at DHS, told the Senate Rules Committee last week. The commission plans to release detailed plans from all states next month.