NEWSLETTER

Morning Cybersecurity

POLITICOPRO

NEWSLETTER

FEDERAL

Cyber 'lifeline' at risk as hackers slam local governments

BY: **DANA NICKEL** | 09/16/2025 05:45 AM EDT

With help from Maggie Miller

DRIVING THE DAY

— Hackers are hammering state and local governments, and the expiration of a key cyber funding program could only make the fallout worse.

HAPPY TUESDAY, and welcome to MORNING CYBERSECURITY! Back in your inboxes with another matcha review. I recently tried Blue Bottle Coffee's iced matcha latte near Union Market. I gave it 3 out of 5 stars: The price-to-size ratio was too high for me, but the taste was refreshing. Where should I go next? Drop me a line at dnickel@politico.com.

Follow POLITICO's cybersecurity team on X at @RosiePerper, @johnnysaks130, @delizanickel and @magmill95, or reach out via email or text for tips. You can also

follow @POLITICOPro on X.

Introducing Global Security, POLITICO Pro's new weekly briefing connecting Washington, Brussels and beyond. Each edition delivers the policies, budgets and industrial shifts shaping transatlantic defense. Add it now: ***Go to Account Settings → Select Defense → Then Global Security.***

TODAY'S AGENDA

POLITICO holds its AI & Tech Summit. 8 a.m.

The House Judiciary Crime and Federal Government Surveillance Subcommittee holds a hearing on "Unmanned and Unchecked: Confronting the Rising Threat of Malicious Drone Use in America." 2 p.m.

The Senate Judiciary Crime and Counterterrorism Subcommittee holds a hearing on "Examining the Harm of AI Chatbots." 2:30 p.m.

HACKED

HELD HOSTAGE — A spate of ransomware attacks in recent months targeting state and local governments in Nevada, St. Paul, Minnesota, and Uvalde, Texas, is heightening concerns about what might happen if key federal programs, such as the State and Local Cybersecurity Grant Program, are not renewed by the end of this month.

"The funding provided by those grants is a lifeline to many under-resourced and underserved populations," said Randy Rose, vice president of security operations and intelligence at the Center for Internet Security.

— Across the country: While not as flashy as some of the other recent ransomware attacks that targeted a massive health care system or a software provider for millions of

students, these recent hacks have caused serious interruptions for residents across several states.

In Uvalde, Texas, schools were forced to close their doors to recover from a ransomware attack that disrupted systems late last week.

This comes just weeks after hackers targeted the state of Nevada in an attack last month, shutting down critical state networks such as the state's Department of Motor Vehicles, causing closures across the state. And in July, officials in St. Paul, Minnesota, announced that hackers cut off access to critical services, such as online water bill payments.

Ransomware attacks can cripple state and local government systems, and cost these organizations more than $2 million in recovery efforts last year, according to research from cybersecurity firm Sophos.

There is valuable data "stored on systems that don't have the most robust security defenses in place," Rose explained. "State and local organizations are 'target rich and resource poor.'"

— Reauthorization on the horizon: The federal government has offered some assistance to states and localities in combating these types of attacks through the SLCGP.

The program provides funding to entities across state and local governments to boost cyber efforts to defend critical infrastructure, including education and government services.

But Congress has less than two weeks to decide whether to reauthorize the cornerstone legislation, which is set to expire on Sept. 30.

"Without those financial resources, many organizations, especially smaller and more rural ones, will have no option but to stop implementing their cyber defenses, leaving their systems, data and constituents at an increased risk," Rose told your host.

A key feature of the program is the coordination it provides between state and local governments, according to Meredith Ward, deputy executive director of the National Association of State Chief Information Officers. Ward told your host that the coordination has been crucial amid serious cuts to federal cyber programs and agencies, such as CISA. And any additional cuts, she said, would affect local governments that are already major targets for hackers.

Despite these cuts, CISA has been working with Nevada officials on incident response in the wake of the August ransomware attack, including helping restore critical services. Still, the onus is being placed largely on states to keep their guards up.

"States hold the primary responsibility for safeguarding their systems," said Marci McCarthy, head of public affairs for CISA, adding the agency has "cybersecurity experts embedded in communities nationwide, offering a wide range of no-cost services to protect governments' networks and critical services."

Another spokesperson for the agency told your host the agency has been "in contact" with officials in St. Paul following the July ransomware attack, but declined to comment on whether CISA is actively working with officials in St. Paul or Uvalde to respond to recent attacks.

— View from the Hill: On Capitol Hill, lawmakers have mobilized efforts in the House to renew SLCGP.

Earlier this month, the House Homeland Security Committee voted near unanimously to advance a bill that would extend the program. The bill is called the Protecting Information by Local Leaders for Agency Resilience Act, or PILLAR Act. It was sponsored by Rep. Andy Ogles (R-Tenn.) and would reauthorize the program for a decade, though it also included language that puts a larger burden on states and localities to help fund this effort than the original law did.

A spokesperson for Ogles did not respond to a request for comment about next steps for the PILLAR Act.

— But wait, there's more: Ransomware attacks are just the tip of the iceberg for state and local organizations, according to Ward.

Ward told your host that state governments are also dealing with cyberattacks boosted by artificial intelligence, and they are regularly targeted by state-sponsored hacking gangs linked to China, Russia, Iran and North Korea.

And without federal policies in place, such as the SLCGP, states will largely be forced to fend for themselves."No state can fight these attacks alone," Ward said. "If one state is attacked, it's likely that other state and local governments will also be attacked."

ON THE HILL

QUESTIONS, CONCERNS — Senate Intelligence Committee ranking member Mark Warner (D-Va.) and Senate Rules Committee ranking member Alex Padilla (D-Calif.) have expressed serious concern that Director of National Intelligence Tulsi Gabbard may have halted intelligence gathering on data around foreign interference in U.S. elections.

In a letter sent to Gabbard on Monday, the lawmakers said that Gabbard has not released an declassified version of the intelligence community's security assessment of the 2024 U.S. elections, and that election security efforts in both the intelligence community and at CISA have been frozen or shut down in recent months.

They urged Gabbard to ensure agencies brief senators on current foreign cyber and disinformation-related threats to U.S. elections before Oct. 10, as well as on planned steps by the ODNI to combat these threats ahead of several key elections taking place across the country.

Olivia Coleman, press secretary for ODNI, called the letter "factually wrong and an obvious effort to spread manufactured panic."

"As we've said publicly on numerous occasions and as Congress has been told directly, all core functions and expertise to ensure the safety, security, and freedom of the American people, including operations to counter foreign and cyber election threats, have not and will not be affected by our ODNI 2.0 efforts," Coleman said.

WATCHING THE WATCHDOG — A dozen Democratic lawmakers are calling on a federal appeals court to uphold a privacy and surveillance watchdog's independence by prohibiting President Donald Trump from firing its members.

In an amicus brief filed on Friday and announced on Monday, Sens. Ron Wyden (Ore.), Ed Markey (Mass.), Rep. Zoe Lofgren (Calif.) and others argued that Trump's firing of

two Privacy and Civil Liberties Oversight Board members earlier this year violates the watchdog's independence and effectiveness.

"No longer could Congress reliably conclude that the PCLOB's reports and recommendations are nonpartisan, independent and guided only by the facts, undermining its value as a legislative aid," the members wrote.

— Zoom out: In May, a D.C.-based U.S. district judge ruled that Trump's firings of Ed Felten and Travis LeBlanc, two Democratic members of the PCLOB, were unlawful, stating that the board's structure was intended to have a restriction on the president's removal power.

The Trump administration has appealed the ruling and plans to argue its case next month before the U.S. Court of Appeals for the District of Columbia Circuit.

CYBER POLICY

DON'T FORGET ME — House Homeland Security Chair Andrew Garbarino (R-N.Y.) is urging Congress to reauthorize the 2015 Cybersecurity Information Sharing Act before its Sept. 30 deadline — despite possible hurdles in the Senate.

"With the statute's sunset date quickly approaching, Congress must act swiftly and decisively to ensure there is no lapse," Garbarino told your host in a statement on Monday.

Garbarino's version of the CISA 2015 renewal, the Widespread Information Management for the Welfare of Infrastructure and Government Act, advanced out of the House Homeland Security Committee markup earlier this month. It included minimal changes to the original bill, which incentivizes cyber threat sharing between the private and public sectors.

— What's next: The Senate Homeland Security Committee is slated to mark up Chair Rand Paul's (R-Ky.) version of the reauthorization on Thursday. Your host scooped last week that Paul's bill includes provisions that remove legal safeguards to incentivize cyber

threat intel sharing, such as cutting Freedom of Information Act exemptions for participating companies.

QUICK BYTES

EYES EVERYWHERE — Elizabeth Daniel Vasquez, a former public defender in New York City and Washington, D.C., writes in an op-ed for The New York Times that the NYPD is showing the U.S. how to use technology to track and surveil Americans.

GONE BUT NOT FORGOTTEN — The FBI recently disrupted a criminal network of botnets, but cybercriminals are quickly picking up the pieces, Robert McMillan reports for The Wall Street Journal.

HELPING HAND — Reuters' Steve Stecklow and Poppy McPherson set out to create an effective phishing scam, and major AI chatbots were happy to help them do it.

Chat soon.

Stay in touch with the whole team: Rosie Perper (rperper@politico.com); John Sakellariadis (jsakellariadis@politico.com); Maggie Miller (mmiller@politico.com), and Dana Nickel (dnickel@politico.com).

AUTHORS

Dana Nickel

YOUR ACCOUNT MANAGEMENT TEAM

James Bambara
Associate Director, BDA Management
jbambara@politico.com