BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

May 22, 2020

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
The Capitol
Washington, DC 20515

Dear Madam Speaker:

We write to thank you for your leadership during the COVID-19 pandemic. As our constituents look to the Federal government for direction and support, you have made clear that Congressional Democrats will not leave those suffering the harsh consequences of the pandemic to fend for themselves. For that, we are grateful.

We are proud that the legislation passed by Congress to address the COVID-19 pandemic incorporated the values that Democratic Members have long championed. Under your leadership, Congressional Democrats have secured funding to help struggling small businesses stay afloat, assist those who have lost their jobs, and invested in the capacity of healthcare providers to ensure access for those who need it. Most recently, H.R. 6800, the *Health and Economic Recovery Omnibus Emergency Solutions Act* (HEROES Act), would provide over $1 trillion of desperately needed aid to state and local governments, including over $3 billion to ensure safe, secure, and auditable elections.

While H.R. 6800 would provide state and local governments important resources, we are disappointed that it did not provide targeted assistance to bolster network capacity and security to ensure that the aid the House provided to displaced workers, frontline workers, and other vulnerable populations is delivered in a timely way. State unemployment websites have been overwhelmed by the unprecedented onslaught of new applicants, resulting in hours-long wait times to access online applications and website crashes.[1] Meanwhile, bad actors with access to previously stolen personally identifiable information (PII) are defrauding state unemployment systems by filing false claims.[2] Unfortunately, states lack the capacity to screen for fraudulent

[1] Jason Knowles, “Illinois Unemployment: Login Problems, Long Waits, Other Issues Persist as Thousands Apply for Benefits,” *ABC7, WSL-TV* (May 7, 2020), https://abc7chicago.com/unemployment-illinois-il-benefits-ides/6161254/; Lorraine Mirabella, “Maryland Speeds Up Processing of Unemployment Claims While Reducing Wait Times,” *The Baltimore Sun* (May 5, 2020), https://www.baltimoresun.com/coronavirus/bs-md-unemployment-claims-improvements-20200505-brym5sqohfaw7naa54jud34ckm-story.html; “Matthew Haag, “They Filed for Unemployment Last Month. They Haven’t Seen a Dime.” *The New York Times* (Apr. 17. 2020), https://www.nytimes.com/2020/04/17/nyregion/coronavirus-pandemic-unemployment-assistance-ny-delays.html.
[2] Mike Baker, “Feds Suspect Vast Fraud Network Is Targeting U.S. Unemployment Systems,” *The New York Times* (May 17, 2020), https://www.nytimes.com/2020/05/16/us/coronavirus-unemployment-fraud-secret-service-washington.html.

applications by identifying multiple applications from the identical web address or using the same bank information.[3] Together, these issues are undermining the good work House Democrats have done to deliver aid to those struggling, delaying aid to those who need it and exacerbating financial challenges facing state governments, including those hardest hit by COVID-19 from Washington to Rhode Island, and Massachusetts to Florida.

Unfortunately, there is more. A week ago, the State of Illinois confirmed a data breach of its new Pandemic Unemployment Portal.[4] In March, a ransomware attack at Champaign-Urbana Public Health District temporarily disabled its public facing webpage and suspended employee access to medical files.[5] Hackers have also exploited the COVID-19 pandemic to create fake websites – typically associated with financial assistance – to steal log-in credentials and PII.[6] Two agencies in Texas have been hit by ransomware attacks this month, which follows a string of ransomware attacks against 22 towns in Texas last summer.[7] These opportunistic attacks are likely to continue as states and localities navigate the COVID-19 response in the months to come.

Toward that end, the implementation of robust tracing capabilities will create new opportunities for bad actors to breach state and local networks. Tracing application developers are rushing to push their products to market. Hastily developed applications may have coding and architecture issues or fail to fully integrate security, creating new cyber risks. State and local governments are rapidly hiring and training people to perform contact tracing work, many of whom may be working remotely, and they must be trained on how to protect the sensitive information they collect.

We would also note that the Cybersecurity and Infrastructure Security Agency (CISA) has repeatedly warned about threats posed to state and local governments by advanced persistent threat (APT), typically backed by foreign governments such as Russia, China, Iran, and North Korea. Before the COVID-19 pandemic, for example, CISA warned that Federal resources would be required to defend against the growing threat to state and local networks triggered by escalated tensions with Iran.[8] Since then, CISA and its partner in the United Kingdom, the National Cyber Security Center, warned that APT groups are "exploiting the Coronavirus Disease 2019 (COVID-19) pandemic as part of their cyber operations" by targeting "healthcare bodies, pharmaceutical

[3] Krebs on Security, "U.S. Secret Service: 'Massive Fraud" Against State Unemployment Insurance Programs,'" (May 16, 2020), https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/.

[4] Lauren Baker, "IDES Confirms Data Breach Within New Unemployment Portal," *WREX.COM* (May 17, 2020), https://wrex.com/2020/05/17/ides-confirms-data-breach-within-new-unemployment-portal/.

[5] Benjamin Freed, "Amid Coronavirus Scare, Ransomware Targets Public Health Agency in Illinois," *StateScoop* (March 12, 2020), https://statescoop.com/amid-coronavirus-scare-ransomware-targets-public-health-agency-illinois/.

[6] "Ready-made COVID-19 Themed Phishing Templates Copy Government Websites Worldwide," Proofpoint blog, (May 14, 2020), https://www.proofpoint.com/us/blog/threat-insight/ready-made-covid-19-themed-phishing-templates-copy-government-websites-worldwide.

[7] Associated Press, "Transportation Agency Hacked in 2nd Texas Government Attack," *The Washington Post* (May 17, 2020), https://www.washingtonpost.com/business/technology/transportation-agency-hacked-in-2nd-texas-government-attack/2020/05/17/f52d52c4-9887-11ea-ad79-eef7cd734641_story.html.

[8] Benjamin Freed, "Iran Tension 'Heightened Awareness' for State and Local Cybersecurity, CISA Chief Says," *StateScoop* (Jan. 23, 2020), https://statescoop.com/iran-tension-heightened-awareness-for-state-and-local-cybersecurity-cisa-chief-says/.

companies, academia, medical research organizations, and local governments."[9] We cannot leave cash-strapped state and local governments to defend themselves against sophisticated hackers backed by foreign governments. Defending state and local governments against foreign adversaries is a Federal responsibility.

It is clear that the challenges posed by the COVID-19 pandemic are far from over. We must equip state and local governments to respond and recover. That means modernizing the architecture of state and local networks so they have the capacity to absorb increased traffic associated with making more services available online and securing the networks to ensure confidentiality, integrity, and availability. Under no other circumstance would we expect a state or local government to defend itself from an attack from a foreign adversary like Russia, China, Iran, or North Korea. Defending state and local networks from cyber attacks should not be an exception.

We support the significant assistance H.R. 6800 provides to state and local governments. That funding is critical to thwarting pandemic-induced economic collapse and ensuring safe, secure, and auditable elections in November. We cannot, however, expect state and local governments, who are being forced to lay off public safety and other vital frontline workers, to choose to invest such funding in cybersecurity over other pressing needs. Given the national security interests associated with a secure Internet ecosystem within government networks, we must provide state and local government targeted funding for IT modernization and cybersecurity.

Once again, we thank you for your leadership and the hard work you have done to ensure that the COVID-19 response packages have reflected the values of the Democratic Caucus. Moving forward, we urge you to prioritize dedicated cybersecurity and IT modernization funding for state and local networks to ensure that the full potential of the resources Democrats have fought hard to provide is realized.

Thank you for your consideration.

Bennie G Thompson

Bennie G. Thompson
Chairman
Committee on Homeland
Security

Cedric L. Richmond
Chairman
Subcommittee on
Cybersecurity, Infrastructure
Protection, and Innovation
Committee on Homeland
Security

James R Langevin

James R. Langevin
Member of Congress

[9] US-CERT, "APT Groups Target Healthcare and Essential Services," Alert (AA20-126A) (May 5, 2020), https://www.us-cert.gov/ncas/alerts/AA20126A.