RICK SCOTT
FLORIDA

ARMED SERVICES
HOMELAND SECURITY
BUDGET
SPECIAL COMMITTEE
ON AGING

United States Senate

July 21, 2023

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Wray:

I write to you today regarding recent reports of a large data breach targeting sensitive personal records of more than one million Floridians, and urge you to prioritize the FBI's investigation of this malicious cyberattack to identify, arrest and prosecute the perpetrators.

As you are likely aware, administrators at Tampa General Hospital detected suspicious activity earlier this year that revealed an unauthorized third-party had unlawfully accessed the hospital's computer systems. Initial reports indicate the hackers carried out the cyberattack over a three-week period, and potentially accessed the records of more than 1.2 million people before the hospital's cybersecurity team was able to intervene. Although the hospital's electronic medical record system was, fortunately, not involved in the data breach, the hackers were nonetheless able to access files containing sensitive personal identifying information that could be used for further criminal activity if the individuals responsible for the attack are not quickly apprehended by your agents. As such, I urge you to assign all necessary resources at your disposal to prioritize the investigation of this incident, and ask that you keep my office apprised of your progress.

Unfortunately, this was not the first cyberattack to target our health care institutions, nor is it likely to be the last unless we prioritize the investigation, arrest, and prosecution of these hackers. In 2021, Scripps Health in California was the victim of a ransomware cyberattack when hackers stole 150,000 patient records.[1] In 2022, the second-largest nonprofit U.S. hospital chain, CommonSpirit Health, was involved in a ransomware cyberattack affecting critical health care services at locations across multiple states.[2] A cyberattack in 2021 on St. Margaret's Health in Illinois disrupted the

[1] https://www.nbcsandiego.com/news/local/what-we-know-about-scripps-health-cyberattack/2598969/

[2] https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/

hospital's billing systems for months, and ultimately contributed to the facility being shuttered shortly thereafter, which has a devastating impact on the community's access to health care services.[3]

The United States is not alone in these cyberattacks as hackers have targeted health systems in other countries. The United Kingdom's National Health System had a ransomware cyberattack in 2017, which led to 19,000 appointments being canceled and 200,000 computer systems being locked out.[4] Late last year, the premier hospital in New Delhi, India, had to shut down their servers for two weeks after a cyberattack.[5]

We know that several of these cyberattacks come from groups operating in (and likely with the approval of) malign foreign states, like Communist China, Russia, and North Korea. In 2014, a cyberattack by Chinese hackers targeting Community Health Systems, which runs more than 200 hospitals in 29 states, stole more than 4.5 million patient records.[6] The Department of Justice has charged Chinese nationals in the past for their involvement in cyberattacks on university and government systems.[7] The Cybersecurity & Infrastructure Security Agency has issued multiple notices on Communist China state-sponsored hackers who have exploited security vulnerabilities and are trying to breach critical systems.[8]

These cyberattacks pose a clear and present threat to our critical health care systems, and so I request your responses to the following questions:

- What is the FBI doing to coordinate with health systems to prevent cyberattacks?
- What is FBI doing with health systems to coordinate investigations after a cyberattack?
- Does the FBI believe that the majority of these cyberattacks are coming from outside of the country?
    - If so, have you identified particular countries from which such cyberattacks are likely to originate?
    - In the past 10 years, how many cyberattacks investigated by the FBI have originated in Communist China, Russia, or North Korea?

[3] https://www.yahoo.com/lifestyle/illinois-hospital-first-health-care-172543050.html

[4] https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

[5] https://www.reuters.com/world/india/indias-leading-state-hospital-recovers-systems-after-cyber-attack-2022-12-06/

[6] https://kffhealthnews.org/morning-breakout/health-it-data-breach-community-health-systems-china/

[7] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

- Does your agency have sufficient resources to fully investigate and pursue the perpetrators of these cyberattacks?
    - If not, what additional resources or authorities are needed?

I urge you to prioritize the investigation of this recent cyberattack against Tampa General Hospital, and hope you will assign all resources necessary to identify, apprehend and hold accountable the hackers responsible. I appreciate your prompt attention to this matter.

Sincerely,

Rick Scott
United States Senator