our networks as basic good cyber hygiene was actually a security breach.

This technique and the breadth of this hack are both unprecedented, and it shows that the Federal Government is still far from where we need to be to handle the cyber security challenges of the 21st century.

As the Permanent Subcommittee on Investigations said in its investigation and report, these alarms that we have been raising over time are ones that we should have paid attention to. In 2019, last summer, Senator CARPER and I issued a shocking report that detailed the unacceptable cyber security vulnerabilities in the Federal Government—vulnerabilities that may very well have played a role in the extent of this breach.

Our report looked back at how well Federal agencies complied with basic cyber security standards over the past decade. Every agency we reviewed failed. And we know that four of those agencies—the Department of Homeland Security, the State Department, the Department of Agriculture, the Department of Health and Human Services—are among those that have been breached in this current cyber attack.

That report from the Permanent Subcommittee on Investigations made clear that Federal agencies were a target for cyber criminals and other nation-state adversaries. In 2017 alone, Federal agencies reported 35,277 cyber incidents. It is the most recent data we have—in 1 year. The number of cyber incidents in 2019 was a little bit less, 28,581. But 2020 will bring what is likely the biggest, most comprehensive breach across the Federal Government in our history.

We also found we are not equipped to handle this threat. Many of the agencies we reviewed didn't even know what applications and platforms were operating on its systems. That begs the question: How can you protect something if you don't even know what you need to protect?

If Federal agencies fail at meeting basic cyber standards, there is no way they are equipped to thwart the kind of sophisticated attack that apparently happened over the past several months. Here, the attackers were meticulous and had a detailed understanding of how to evade intrusion detection practices and technologies. And because the Federal agencies involved were unprepared, the attackers had ample time to cover their tracks, which means evaluating the extent of the damage and kicking them off our networks is going to be incredibly difficult and time-consuming.

Given how widespread this attack is and how much wider it is expected to become, it certainly seems like the Federal Government's current cyber resources are going to be spread incredibly thin.

Congress and the executive branch have failed to prioritize cyber security, and now we find ourselves vulnerable and exposed. We have to do better than this. This breach has to be a wake-up call for all of us.

Over the years, I have worked across the aisle with Senator PETERS, Senator CORNYN, Senator HASSAN, and others on legislation to beef up our Federal Government cyber capacities, including the Risk-Informed Spending for Cybersecurity Act, the Federal System Incident Response Act, and the DHS Cyber Hunt and Incident Response Team Act, and others. We are proud of this legislation.

Let's be honest. It wasn't enough. We need to do more. We need to not only defend our networks but go on the offense to defer a nation-state, like Russia, and nonstate actors from even considering a future attack like this. That means there needs to be consequences for cyber attacks significant enough to prevent them from happening again and a willingness to act preemptively when warranted.

Congress has to take a hard look at the cyber security capabilities of our Federal agencies. In the next Congress, I will be the top Republican on the Senate Homeland Security and Governmental Affairs Committee, which means I will either serve as its chairman or ranking member, depending on the outcome of a couple of races in Georgia. Senator PETERS will be the chair if the Democrats take the majority. I will tell you here tonight, whether I am chairman in January or him, we intend to hold indepth hearings on cyber security. With what has happened, we will also, of course, focus on the origin, scope, and severity of this breach.

Actually, 3 weeks ago, even before this attack was revealed, we met and decided to hold these cyber security hearings, and we are already working on comprehensive legislation to improve our cyber defenses in the Federal Government going forward.

We must now move with a renewed sense of purpose and urgency to learn from this massive attack. We have to remove these hackers from these systems and put in place protections to prevent it from happening again.

As this cyber attack has made clear, we have to redouble our efforts to shore up our defenses. We are two decades into the 21st century, but most of the Federal Government legacy computer systems are from the 20th century. Federal agencies are simply behind the times when it comes to defending themselves against these threats posed in cyber space. The government is trying to respond to sophisticated, 21st century attacks with 20th century defenses. This attack has shown us the consequences of that and should be the catalyst for real bipartisan action here in the next Congress to better defend networks that contain sensitive, personal information, and other information critical to our economy, our healthcare, and the safety and security of all Americans.

I yield the floor.

The PRESIDING OFFICER (Mr. TILLIS). The Senator from Ohio.

Mr. PORTMAN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. BENNET. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

CORONAVIRUS

Mr. BENNET. Mr. President, before I give my remarks, I would like to say that I hope the rumors are true that we are getting close to a deal here. The country needs us to reach a bipartisan deal, as we did in March, unanimously, when we passed the CARES Act here.

It is time for us to do that again. In Colorado and all across the country cases are spiking and the economy is slowing down. People need relief. They need help. I hope we will come together in a bipartisan way and do that.

I hope that the deal is not going to come crashing down because of a disagreement about what the Federal Reserve's authority ought to be under the 13(3) program. That is an important program for the Federal Reserve to help when things are really distressed in our economy—to help our small businesses, our State and local governments, and working families all over this country.

It is an authority that Donald Trump used—or that the Fed used while Donald Trump was President. People on both sides of the aisle said it was an effective authority, and if it is an effective authority for President Trump, it should not be taken away from the Federal Reserve just because Joe Biden is becoming President of the United States.

So I hope that we will come to an agreement. I expect that we will. I hope it is soon. People need the help.

CYBER SECURITY

Mr. President, in the last few days we have learned that the United States was subject to one of the most brazen cyber hacks in history. Based on press reports alone, the hackers appear to have breached the Department of State, the Department of Commerce, the Department of Energy, the Department of the Treasury, the National Nuclear Security Agency, and the Department of Homeland Security—including the agency responsible for our cyber security.

On top of that, the hackers also managed to breach major American companies like Microsoft and compromised several State governments and other foreign governments all at the same time in this process.

While we are learning more about these breaches, the level of resources and sophistication bears all the hallmarks of Russia. Reports suggest that the hackers have been in the system since the spring and perhaps much longer. According to public reports, they may still be in our system tonight.