Statement by Senator Susan M. Collins
Cyber Incident Notification Act of 2021
July 22, 2021

Thank you, Mr. President. First, let me thank my good friend and the leader of the Senate Intelligence Committee, Chairman Warner, for paving the way for this legislation. He cares deeply about our country's response to these terrible cyberattacks and intrusions. And I am so grateful for his leadership and for his working with me to produce the *Cyber Incident Notification Act of 2021*. As the Chairman has mentioned, this is a bipartisan bill. It is broadly supported, and it would strengthen our response to cyberattacks and thus help to prevent future cyber intrusions. It would require government agencies, federal contractors, critical infrastructure entities—which are overwhelmingly owned and operated by the private sector—and other important sectors, to notify the U.S. government if they become the victims of a significant cyber attack or intrusion.

This effort, Mr. President, is a direct outgrowth of our work on the Senate Intelligence Committee and reflects our long standing concern regarding the lack of timely notification of cyberattacks that can lead to extremely serious consequences for our economy, for our national security, and for our individual privacy.

Mr. President, in September of 2019, for example, Russian hackers gained access to the Solar Wind software. This resulted in a supply chain compromise that was downloaded by up to 18,000 of its customers. These hackers then conducted follow on operations that compromised nine federal agencies and 100 private sector networks. We did not become aware of this hack until more than a year later. And only then, because a cybersecurity firm called Fire Eye voluntarily notified the federal government and the public.

Mr. President, just to reiterate that important point, Fire Eye was under no legal obligation whatsoever to tell us that the software had been compromised, even though it affected nine federal agencies. We are grateful that Fire Eye told us about this hack. But the fact that companies are not mandated to do so leaves our economy and national security vulnerable to future attacks, and lessens our ability to respond effectively when such intrusions do occur. Where would we be right now if Fire Eye had not voluntarily disclosed the intrusion? Would the Russian operations still be ongoing? How much sooner would we have become aware of these Russian cyber operations if key sectors were required to report cyber incidents to the U.S. government?

As the Senator from Virginia very kindly and generously noted, I have long been concerned about this problem and focused on it. In 2012 when I was the Ranking Member of the Senate Homeland Security Committee, I joined with my Chairman and dear friend, former Senator Joe Lieberman of Connecticut, in introducing a bill called the *Cyber Security Act of 2012*. That bill would have, among other things, addressed this gap in cyber incident reporting. Unfortunately, our bill did not become law. How much more prepared we would be today if it had been enacted.

My 2012 bill would have led to improved information sharing between the private sector and the federal government. That likely would have reduced the impact of cyber incidences on both the government and the private sector. Having a clear view of the dangers the nation faces from cyberattacks is necessary to enable both the public and the private sector to mitigate and reduce the threat. We've just recently seen the impact of an attack on a major pipeline—just think what the consequences would be of an attack that crippled our electric grid.

Mr. President, what we are proposing, the *Cyber Incident Notification Act*, is common sense and long overdue. Our bill recognizes the additional burden that this reporting requirement places on parts of the private sector, and so it therefore provides additional liability protection for companies reporting cyber incidents and requires the government to harmonize these new mandates with any existing reporting requirements to help avoid duplication. The bill also requires the government to produce analytic updates for the government and industry practitioners regularly so that they are aware of cyber incidents taking place and targeting their sectors. This should be a two-way street of the exchange of information.

Mr. President, let us not delay any longer in passing a robust cyber incident notification requirement. Failure to pass this bill will only give our adversaries more opportunity to gather intelligence on our government, to steal intellectual property from our companies, to compromise our personal privacy, and most of all, to harm our critical infrastructure. Thank you, Mr. President.

Mr. President, I would yield the floor…again, my thanks to the Senator from Virginia, the Chairman of the Intelligence Committee, for his hard work on this bill. Let's get the job done. Thank you.