Senator Charles E. Schumer
Statement and Questions for the Record
Ransomware Hearing
May 18, 2016

I want to thank Senators Graham and Whitehouse for convening this hearing today and calling attention to this increasingly important issue that all too often flies under the radar. In fact, the first time many people hear of ransomware is when they become victims. If we are going to put a stop to the problem that has to change; hearings like this are an important step in that direction.

I have a particular concern about ransomware due to several recent attacks on institutions and municipalities in my home state of New York. According to the *Utica Observer Dispatch*, the Village of Ilion in Herkimer County paid $800 just two years ago to regain control of its computer systems. In March of this year, in the Town of Manlius, a town employee's computer was attacked by hackers from Crimea, Russia. Luckily, the town had purchased cybersecurity insurance, and employees were trained in what to do if they suspected an attack. According to the *Post Standard*, the town's IT department was able to thwart the threat by taking the computer off the system before the entire network could be impacted. In 2015, according to the *Times Union*, the Capital Region Chamber of Commerce pulled down its website following messages from members reporting that they were receiving alerts that their data had been locked and hackers were demanding cash in exchange for retrieving it. In addition, one hospital and a community center in the Capital Region reported being attacked by ransomware.

These are a few examples, but they are far from the only ones. Many municipalities, hospitals, schools and banks have lost vital capital and resources to cyberthieves who have infiltrated their networks and held critical data hostage. Given the increasing number of these incidents in recent months, both in New York and across the country, I want to urge the administration to redouble its efforts to put a stop to ransomware.

Stopping ransomware is not just about pursuing the perpetrators, which should be done aggressively. It is also about preventative defense. We need more resources on the federal, state and local level being dedicated to IT infrastructure upgrades, cyber hygiene, and proper training so that ransomware cannot take hold in the first place.

Questions for Mr. Downing:

- Can you tell me about what kind of efforts the federal government is taking to prevent ransomware attacks?
- How are you working with under-resourced state and local governments to ensure they do not become victims.
- Would you support increased funding for state and local governments to improve their IT infrastructure and prevent cyberattacks – whether ransomware or any other variety?
- The President set up a Cybersecurity Commission as part of his Cybersecurity National Action Plan. Do you agree that this Commission should make ransomware prevention a key focus of its investigation and recommendations?