Judiciary Subcommittee on Privacy, Technology, and the Law Hearing on "Equifax: Continuing to Monitor Data-Broker Cybersecurity"
October 4, 2017
Questions for the record for Jamie Winterton and Tyler Moore
by Senator Whitehouse

(1) Federal government cybersecurity responsibilities are currently spread across 73 different Inspectors General, and many of these offices lack the expertise or the capacity to do more than simply check compliance with minimum standards. In your view, what are the national security implications of this fragmented oversight of the federal government's cybersecurity?

One unique aspect of cybersecurity threats is that they evolve exceptionally quickly. How do we address problems that change so rapidly with such a dispersed governance structure? To prevent surprise and ensure complete coverage of our threat surface, we need a tightly knit organization that can address new problems rapidly and thoroughly. That's difficult to do with so many pieces.

It's often said that defense needs to move at the speed of attack – this is true not just for cyber technology, but the accompanying policy and regulation. We have a long way to go, but establishing communication between these entities and shared minimum capacity requirements would be a good initial step.

(2) Few non-specialists truly understand our vulnerability to a wide range of cyber threats, from hacking and the theft of private data to cyber attacks on critical infrastructure like public utilities or the banking system. Often, information about cyber attacks is reflexively classified, which denies the American people – not to mention state and local governments – an adequate awareness of the threat. Do you believe increased transparency with respect to our cyber threats and vulnerabilities would enhance national security? If so, do you have any recommendations as to how to safely and effectively increase it?

Let's first consider what "adequate awareness" means for individuals and for decision-makers. Right now, individuals are expected to be specialists in protecting themselves – the onus of responsibility is, in my opinion, too high. It's as if an individual driver were required to build their own seat belt every time they sat in the driver's seat of a car, and were punished for not understanding how all the pieces work, or not building it correctly every time. We need to make security more accessible for individuals so they can use technology without fear that it will harm them.

"Adequate awareness" for decision-makers, however, requires a realistic understanding of the threat landscape, how different populations are affected by cyber-threats (e.g., elderly people or children, critical infrastructure, utility companies). I can't speak directly to the classification issue, since my clearance is not currently active – but data sharing programs and large-scale analytics of cyber-threats are essential in predicting new threats and protecting against them. A realistic understanding of threats and vulnerabilities also combats the "fear, uncertainty, and doubt" (FUD) model often used by vendors to hype problems and peddle weak solutions.

(3) At this point, we lack the data necessary to determine whether the NIST Framework is

popular because it demands so little or because it produces better cybersecurity outcomes. What recommendations do you have for stress-testing the Framework to ensure that it is producing adequate security?

According to Gartner, 30% of US companies currently use the NIST cybersecurity framework, including all of the top 10 companies in the Fortune 500. The NIST framework does not on its own solve cybersecurity problems, but it provides a way for a company to understand its' threat surface. For additional industry perspective, I reached out to Kim Jones, a colleague with 20 years of CISO experience. In Kim's experience, the NIST framework is valuable because it facilitates a discussion on how much risk an organization faces and how that risk can be mitigated. A business using the NIST framework can "decide upon its risk posture, then evaluate the existing and needed protection posture accordingly."

The Framework is a bit like antibiotics. The medicine may be very effective, but only if taken according to the prescription. Half a dose of antibiotics can actually be harmful, as could a half-adoption of security measures. An assessment of how companies are using the Framework – the choices they make as a result and how (or if) they are propagated throughout the company – would provide valuable insights as to how the Framework should be adopted, promoted, or modified.