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
Responded October 25, 2017

(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?

Taking a holistic approach to cybersecurity policy is essential, as it is an issue that spans many industries, jurisdictions and purviews. In addition to challenges of effective oversight, fragmentation of cybersecurity responsibility means that the federal government's cybersecurity talent is also spread thinly and not used to its full potential. Many of the threats posed to civilian agencies are the same, and the defenses might be more effectively implemented if there were greater cooperation and shared responsibility across agencies.

(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?

I strongly believe in the power of and need for increased transparency regarding cybersecurity threats, incidents, and resulting harms. Because so much of our nation's critical infrastructure is controlled by the private sector, it is essential that the operators of that infrastructure understand the nature and severity of threats so they can manage cybersecurity risks accordingly. To an extent, the sector-specific information sharing and analysis centers (ISACs) help foster information sharing, but this could be strengthened by the government sharing more information with such groups. Often, classifying cybersecurity threat information is not only counterproductive, it can even pose a national security risk.

The public sector can play an essential coordinating role in gathering, aggregating and disseminating data on harms that arise from data breaches and other cybersecurity incidents. Right now, firms are only obliged to disclose that a breach of personal information has occurred. They are not required to disclose other forms of cybersecurity incidents, nor must they share information on resulting harms, such as increased fraud or customer disputes that result from breaches. Firms should be encouraged to share such information voluntarily, but if they do not, then compulsory disclosure may be required. By gathering and sharing information on the prevalence and cost of harms, firms can elect to

devote adequate resources commensurate to the threat.

(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?

The NIST cybersecurity framework emphasizes the process of cybersecurity without regard to outcomes. In one sense, this is understandable because reliable data on cybersecurity outcomes is hard to come by, let alone information that quantifies the relationship between adopting various controls and cybersecurity outcomes. But the drawback of a process-based approach that emphasizes adherence to controls without evaluating their effectiveness is that we cannot determine if adherence to the framework actually improves outcomes.

I would recommend that organizations be encouraged to voluntarily (and confidentially) disclose their degree of adoption of various controls in the NIST framework. This information could be combined with gathered data on incidents to empirically evaluate the framework's effectiveness, and subsequently to improve the framework and make recommendations for which controls to prioritize.

One aspect of stress-testing that could be readily applied to credit-reporting agencies would be to evaluate the firms' *respond* and *recover* efforts (in the parlance of the NIST framework). It is very clear from the aftermath of the Equifax data breach that the company did not adequately plan for the potential of a large-scale data breach occurring. While it is impossible to prevent all cybersecurity incidents, organizations can be better prepared to deal with the fallout, and this can be evaluated in advance. Credit-reporting agencies should have contingencies in place to ramp up call center staff, roll out defensive countermeasures with acceptable license agreements, use secure websites for messaging, etc. At the very least, regulators should be prepared to evaluate those contingency plans so that when the next breach occurs, the response does not undermine consumer confidence.