Opening Statement – Rep. James Langevin (D-RI)

Subcommittee on Cybersecurity and Infrastructure Protection Hearing

Maximizing the Value of Cyber Threat Information Sharing

November 15, 2017

Two years ago, Congress passed the Cybersecurity Act of 2015 to remove barriers to fuller and faster cybersecurity threat indicator sharing both between government and the private sector and among private entities.

This legislation was the result of years of negotiation between experts from industry, academia, privacy advocates and security professionals. At the time, there was broad consensus that we were not sharing, analyzing, and integrating data around cyber threats as well as we could be.

To answer this gap in our cybersecurity posture, Representatives from both sides of the aisle came together as partners to deliver legislation that removed the legal hurdles that prevented the free flow of threat indicators and to provide liability protections to encourage sharing.

Today, those barriers are gone. There are ironclad authorizations for companies to share indicators within industry and back and forth with the federal government. There are liability protections to ensure that these actions do not inadvertently put companies at risk. There are even protections on the data themselves to ensure that they are not used for any regulatory action by the government.

The Cybersecurity Act of 2015 also created a channel for the government to better disseminate information that would otherwise be classified. By placing these signals amongst the contributions from all participants, DHS can disguise the original sources. During the period of October 2015 to April 2017, the Department has shared 2,290 formerly classified cyber threat indicators through the Automated Indicator Sharing program, or AIS.

However, despite these advancements, we have a long way to go in operationalizing the law and policy that has been developed.

Barely more than 100 companies have elected to join the program and contribute to the common threat picture, a level of participation that is simply unacceptable.

Part of this is on the Department, as we have heard numerous times before this Committee that the indicators shared by the government are often late and lack important context.

But part of this also falls to industry – after all, with only roughly one hundred private sector participants, it seems many people knocking the data being shared by AIS haven't applied much effort to analyzing the data. 2200 formerly classified threat indicators certainly count for something.

That is why I am grateful to Chairman Ratcliffe and Ranking Member Richmond for continuing to study this issue. We need to know what is and isn't working with the law and with the Department's efforts. We also need to know what activities are being enabled that weren't happening before passage of the law and the ironclad authorizations I mentioned.

I have said many times that information sharing is not a silver bullet – in fact, there is no such thing in cybersecurity. But I do believe in its promise to help better our cybersecurity posture, and we in Congress owe it to the American people to ensure we are meeting that potential.

So I will be interested in hearing from the witnesses what we in Congress can do to improve the Department's efforts and to improve uptake among private sector participants.

Personally, I think that we may need some more assistance from the Department in building a robust ecosystem around the feed – rather than just relying on it being out there – and I hope the Department looks to the Financial Sector's experience with Soltra Edge for guidance.

But I also hope that the private sector, innovative as it is, applies some of the creativity to the data coming out of DHS rather than waiting.

Finally, there are two related issues that I want to mention briefly.

First, I believe it will be extremely difficult for the Department to make any lasting changes in its policies without permanent political leadership in place, and I hope the Administration moves swiftly to fill critical vacancies at the National Protection and Programs Directorate. Cybersecurity is a national priority, and the personnel decisions made by the White House need to reflect that.

Second, a brief comment on the new Vulnerabilities Equities Process (VEP) Charter released today. I am grateful that the document continues the presumption of disclosure and ensures a broad array of government stakeholders, including DHS, have a seat at the table when discussing vulnerabilities. I am also pleased by the increased level of transparency indicated by the publication of the Charter in UNCLASSIFIED form and by the annual reports, including to Congress, it requires.

We owe the selfless Americans who serve their nation as members of the Intelligence Community an enormous debt of gratitude, a debt that is far too infrequently acknowledged. As Members of Congress, we also owe them rigorous oversight to ensure the tools they develop remain secure. I believe that the VEP is an appropriate process for selecting the very few vulnerabilities where disclosure will be delayed. However, that process falls apart if the exploits cannot be kept in government hands, and Congress must do more to ensure those safeguards are in place.

With that, I would like to thank the witnesses for being here today, and I look forward to discussing way to improve our collective cybersecurity with them.

# # #