Rep. Yvette D. Clarke (D-NY), Opening Statement as prepared

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

Committee on Homeland Security

Markup of H.R. 3674

February 1, 2012

When it comes to cybersecurity, there has been a bipartisan commitment in this Subcommittee to ask hard questions, support DHS as it executes its cybersecurity missions, and foster greater network security of Federal networks as well as critical infrastructure networks.

As a result of this shared commitment, this Subcommittee has amassed a significant oversight record over the past few years.

Today, the moment has arrived for us to consider legislation that, in large part, reflects this Subcommittee's oversight findings.

Back in December, at the legislative hearing, I stated my belief any cybersecurity legislation to emerge from this Subcommittee should give DHS sufficient authority to help protect Federal networks and foster greater cybersecurity for covered critical infrastructure.

I believe this "Amendment in the Nature of A Substitute" accomplishes those twin goals.

I am particularly pleased that the measure contains provisions similar to the cybersecurity legislation I introduced with Ranking Member Thompson to increase DHS' authorities for the cybersecurity of the Federal government, increase DHS' cybersecurity R&D activities, and direct Federal regulators to update cybersecurity requirements for covered critical infrastructure operators based on DHS-identified risk-based performance-based standards.

Also, I am pleased that Chairman Lungren agreed to authorize the National Cybersecurity and Communications Integration Center as the Federal government's focal point for cybersecurity information sharing and incident response, and include my proposal for a pilot program for cybersecurity for our Nation's fusion centers.

While there is much to like in the first half of the legislation, I continue to have reservations about the main provision in the second half – the "National Information Sharing Organization".

As proposed, the NISO would be a new public-private quasi-governmental entity established for the purposes of information sharing, performing collaborative cybersecurity R&D, and promulgating voluntary cybersecurity standards.

At the December legislative hearing, I raised a number of specific concerns about the NISO proposal.

I am pleased to say that many of my concerns have been addressed in the ANS.

Specifically, I expressed concern that the initial draft included language requiring DHS to pay up to fifteen percent of the NISO's annual operating budget.

I am pleased that the ANS limits the Federal appropriations to $10 million per year for the first three years, as essentially start-up money.

Thereafter, the only Federal money that would flow into the NISO would be the member fees paid by the Federal government, like any other participating organization.

Additionally, I expressed concern about the initial draft's criminal penalties for the impermissible disclosure of NISO information was too narrow—as it only applied to Federal employees.

The bill subjects anyone, be they a Federal employee, a NISO employee, a contractor, or employee of a member, to the same penalties.

Even with these improvements, I have fundamental doubts about establishing this clearinghouse and whether it is the best way to address the growing cyber threats to our country.

Accordingly, I will be offering an amendment to strike and replace the NISO authorization with a requirement that DHS conduct an assessment or survey of clearinghouse options to identify the most effective approaches or models to foster the voluntary sharing of information on penetrations and hacks by the private sector.

Before we commit $30 million of taxpayer dollars on a whole new clearinghouse, shouldn't we take the time to consider whether the NISO, as conceived, is likely to deliver the desired results?

I hope that Members will support my amendment that seeks to ensure we don't put the "cart before the horse."

If my amendment fails and the NISO provision, as drafted, is retained, Members should take note that the broadness of this provision raise serious questions on: how such an organization would actually function, whether the government—as a minority member—can ensure the organization is furthering national priorities, and how its existence would impact DHS' cybersecurity operations.

Today, and in the days ahead, Mr. Chairman, I look forward to working with you to answer these questions, as we advance comprehensive cybersecurity legislation.

Ultimately, Mr. Chairman, I know we share the same goal of getting comprehensive cybersecurity legislation signed into law that gives DHS the authorities and tools it needs to protect our government networks and help foster greater more security for critical infrastructure networks.

Thank you again Mr. Chairman, and once again I look forward to working with you to produce the best legislation possible.