Opening Statement of Rep. Cedric L. Richmond

Ranking Member Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

Joint Subcommittee Hearing - "Wassenaar: Cybersecurity & Export Control"
January 12, 2016

The Wassenaar Arrangement consists of American efforts in collaboration with 40 of our trading partners to put into place export controls for conventional arms and dual-use goods and technologies. As we know, dual-use goods are commodities, processes, or technologies used primarily for civilian purposes, which can also be used to develop or enhance the capabilities of military equipment or initiatives.

We find ourselves in rapidly changing times, and dual-use good and technologies now encompass cybersecurity technologies, which are vital in protecting private, commercial, and government data, and protecting the operation of our information networks, both public and private. The forty-one nations participating in the Wassenaar Arrangement agreed to include cybersecurity issues, and the United States has led the way.

The Department of Homeland Security's Cybersecurity and Communications Office, within the National Protection and Programs Directorate, is the storehouse of a great deal of our nation's civilian cybersecurity expertise, and I'm glad to see Dr. Schneck as one of the witnesses today, and look forward especially to her perspective.

I've found it helpful to frame the cybersecurity issues contained in the Wassenaar Arrangement as a series of questions:

- Does the proposed rule fulfill its intended goal?
- Does the proposed rule have any negative, unintended side effects?
- Will modification of the proposed rule address concerns adequately? And,
- Should the Wassenaar provision be renegotiated or an alternative be found?

According to a large number of professionals, the export restrictions for the defined cybersecurity products and technologies in the rule may certainly reduce the likelihood of repressive governments obtaining surveillance technology through legal sources, but the criminal underground would not be subject to such restrictions, and such repressive regimes might switch to those suppliers. But let us not speculate.

While my Subcommittee does not appear to have any immediate legislative or oversight jurisdiction on this matter, testimony today from industry and the government agencies involved will help us to learn about the impacts of the proposed rule as drafted, and how it will affect or impede, not only research on the specifics of cybersecurity, but possible effects on the larger global cybersecurity community.