



OPENING STATEMENT

January 12, 2016

MEDIA CONTACTS

Susan Phalen, Matthew Ballard

**Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee
House Homeland Security Committee**

Wassenaar: Cybersecurity & Export Control

Remarks as Prepared

The House Homeland Security Committee Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies and the House Oversight and Government Reform Subcommittee on Information Technology meet today to hear from key industry and government stakeholders about the impact the Wassenaar Arrangement will have on the American people, U.S. businesses, and the cybersecurity industry.

First, I want to thank my friend Mr. Will Hurd, the gentleman from Texas, for co-chairing this hearing. Today we are doing what Americans would like to see more of in Congress. Two Committees that don't often get to work this closely are able to – and happy to – come together to tackle an issue that is extremely relevant to national security and the security of individuals' personal information. I believe this is one of our core duties in Congress: to bypass jurisdictional roadblocks and make real progress towards keeping our citizens safe.

Private industry in America is excellent at responding to consumer demands. Many companies, some here today, pride themselves on guaranteeing the security of their customers' personal information. Others represented here exist solely to help in securing that information. They also secure vital sectors of society, such as critical infrastructure and the financial sector. Their success hinges, in large part, on their ability to guarantee their own security.

Today, I hope to hear from our witnesses on how the Wassenaar Arrangement and its implementation would affect these objectives.

The Wassenaar Arrangement was established 20 years ago to apply to conventional arms and dual-use goods and technology. Changes made in 2013 sought to extend export controls to cybersecurity intrusion and surveillance software and technology. These changes were motivated by a desire to prevent authoritative regimes from repressing their people.

This intent is noble. Yet the Administration's implementation effort resulted in united dissent from the technology and cybersecurity industries, academics, and researchers. The energy and financial sectors voiced deep concerns. And they were echoed by civil society groups, who said the proposal could make communicating about security vulnerabilities almost impossible in certain cases.

The federal government engages in countless ways with the American people and our international partners. When proposing actions, the government should – at a minimum – do no harm to its own people.

I am interested to hear from our government witnesses how they believe this arrangement will successfully deter the accumulation of digital weapons, which aren't constructed in factories, don't need physical space for storage, and don't depend on traceable means of transport. I hope to better understand how they believe this export control framework can be effectively applied to intrusion software.

I agree that we should strive to limit dangerous technologies from falling into the hands of bad actors. But national security and Americans' personal security can't be sacrificed. There are many ways the United States strives to combat human rights violators and I hope to hear today about why this route was chosen over other options.

As we can see by the variety and size of the witness panel, the Wassenaar Arrangement has broad implications. Recent reports and the witness testimony today demonstrate that we are far from a consensus on this issue.

The Administration's top three cybersecurity priorities include 1) "protecting the country's critical infrastructure from cyber threats"; 2) "improving our ability to identify and report cyber incidents"; and 3) "engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace." I assume that our government witnesses are well versed in these goals and their prioritization.

Yet in reading comments to the proposed rule and general thoughts on the cybersecurity section of the Wassenaar Arrangement, one sees a probable contradiction of the first two goals. Additionally, it is unlikely that this Arrangement achieves the open and interoperable cyberspace that is in the public's interest. If we are to expect the cybersecurity provisions of this Arrangement to be workable, we need to make sure our stated intentions and actions are not contradictory. If we can't do that, I question why we as a country are agreeing to this updated Arrangement.

Just last month, Congress passed legislation to encourage the sharing of cyber threat information. Both the private sector and the government stand to benefit from the increased flow of valuable cyber threat information. Today, we need to hear whether the Wassenaar Arrangement would have a counterproductive impact on such sharing and whether it would undermine the law that the President just signed.

As a Nation, we advocate for human rights and assist those harmed by authoritarian regimes. However, we must first and foremost safeguard the security of our Nation and our citizens. I look forward to hearing from the witnesses about the path forward and how we can come together to best protect the American people.

###