Statement of
Vann H. Van Diepen
Principal Deputy Assistant Secretary
for International Security and Nonproliferation
U. S. Department of State

Before the

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

And the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

January 12, 2016

Thank you, Chairmen Hurd and Ratcliffe, Ranking Members Kelly and Richmond, and Members of the Committees, for the opportunity to talk to you today about nonproliferation export control efforts in the new area of cyber tools. This is a very challenging area. We hear almost daily about malicious cyber activities that disrupt businesses, compromise privacy, or threaten national security. The 2014 destructive malware attack on Sony Pictures Entertainment and recent high profile intrusions involving the exfiltration of sensitive data from government and private sector computers highlight the kinds of cyber threats we now face. These dangers are only increasing as the tools for carrying out these actions in cyberspace become more widely available and more powerful.

While these cyber tools enable breaches of networks and data for malicious purposes, they can also be used for beneficial purposes, such as identifying vulnerabilities and improving cybersecurity. The private sector and security research community play a critical role in promoting cybersecurity, and it is important that they continue to innovate in this dynamic technological space.

Congress itself has recognized the overall cybersecurity threat that our nation faces, and it has sought to specifically address the dangers posed by the uncontrolled spread of capabilities to carry out malicious activity in cyberspace. In the 2014 National Defense Authorization Act, Congress required the President to develop an integrated policy to control the proliferation of what it termed "cyber weapons" though unilateral and multilateral enforcement activities, financial means, and diplomatic engagement.

To be most effective, export controls should be multilateral; obviously, it is easier to evade just the controls of the United States than those of dozens of countries. The Wassenaar Arrangement has the responsibility for multilateral national security export controls on dual-use items not related to weapons of mass destruction (WMD), such as cyber tools. This 41-country regime was established in 1996 to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms

and related dual-use goods and technologies, thus preventing destabilizing accumulations, including by terrorists.

Over Wassenaar's 20-year history, it has contributed to national and international security by establishing control lists and best practices that have led to its Participating States preventing transfers of arms and sensitive dual-use items to countries and programs of concern. The concerted efforts of its members in controlling the items on its lists, and keeping those lists up to date, is a critical component of U.S. and international security. The Wassenaar control lists, along with those of the WMD and missile nonproliferation regimes, form the backbone of the U.S. dual-use control system.

The United States is a global leader in nonproliferation, including in Wassenaar. We have pressed consistently for controls on a range of dual-use technologies that, when used appropriately, can protect us, but can also be used against us, including things like lasers and sophisticated electronics. When all 41 members, as well as the growing number of non-member countries that adhere unilaterally to Wassenaar controls, work together to control sensitive technologies, we can better keep these items out of the hands of those who would use them against us -- while preserving their use in legitimate trade.

We need to strike the appropriate balance in implementing such controls to promote national security objectives while making sure that the controls' benefits

clearly exceed any commercial or national security costs. Upholding our international export control commitments is central to our ability to get other countries to uphold theirs, not just in Wassenaar but in the WMD and missile control regimes as well.

Recognizing the challenge in implementing the cyber control, the U.S. government took the uncommon step of going through a public notice and comment process. Usually, Wassenaar controls get implemented through a final rule. The U.S. government made this decision because we wanted to give industry and the research community an opportunity to provide their views and wanted to make sure we get U.S. implementation right. The comments were instructive, and we take them very seriously. It is clear from the comments received that the first version of the proposed U.S. rule to implement the Wassenaar control missed the mark, and the interagency continues to work through the concerns raised.

Fortunately, the cyber control is included on the least sensitive portion of the Wassenaar list. This provides us with substantial flexibilities we can employ in the process of implementing that control nationally, just as most other Wassenaar members have done in already having implemented the cyber control for over a year without apparent controversy.

We appreciate your Committees' interests in this issue, and we are committed to working closely with Commerce and all other stakeholders in the

interagency, as well as industry and the other relevant external stakeholders, to seek a balanced way forward that meets our important policy objectives while addressing the concerns raised.