December XX, 2015

The Honorable Susan E. Rice
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear Ambassador Rice:

The Department of Commerce is preparing to issue a proposed rule that has the potential to significantly undermine the United States' cybersecurity posture. We write to share our concern that this rulemaking, which is part of an effort to implement the 2013 additions to the Wassenaar Arrangement pertaining to export controls of "intrusion software," could seriously hinder our national security without a significant overhaul.

The original proposed rule, issued by the Bureau of Industry and Security (BIS), contained flaws that some of us highlighted during the public comment period. The definition of intrusion software, agreed upon by the Department of State at the Wassenaar Plenary, is very broad to the point that it includes a number of products regularly used for cybersecurity research and defense. The definition is so all-encompassing that any implementation must greatly narrow the range of affected technologies; if that proves unfeasible, the language of the Arrangement itself may need to be renegotiated. BIS was cognizant of this challenge when drafting the initial rule; unfortunately, the proposed solution – attempting to draw a line between offensive and defensive cyber tools – was misguided, as defenders need access to exploits to test their networks. This artificial distinction, combined with the lack of a waiver of deemed export rules, could have a chilling effect on research, slowing the discovery and disclosure of vulnerabilities and impeding our nation's cybersecurity. These concerns were echoed by nearly three hundred public comments representing a diverse array of interests. Consequently, after evaluating these comments, we are concerned that BIS may lack the policy expertise to appropriately weigh these critically important security interests.

We agree that the export of sophisticated hacking technologies to criminal organizations or repressive regimes is a legitimate national security concern. However, it is vitally important that the rule created to improve national security – by preventing these software exports – does not itself impair security efforts and we strongly believe the initial rule, as proposed by BIS, would have done just that.

As you know, governmental and private sector networks are under near constant attack from sophisticated adversaries using cutting-edge technologies. To defend against these threats, network operators need real-time access to the best available cybersecurity technologies. The proposed BIS rule would have dramatically reduced our ability to defend our nation's networks – hindering companies' abilities to acquire and utilize new security technologies as well as

impeding vulnerability disclosure and information sharing – while only marginally reducing malicious actors' abilities to use hacking tools.

Throughout the rulemaking process, BIS has been very accommodating to stakeholders, participating in numerous listening sessions and working closely with its Technical Advisory Committees. We believe that clear advice from the Executive Office of the President will help BIS and State put these comments into context. Therefore, we request that you take an active role in collaborating with BIS and State to reevaluate the 2013 Wassenaar additions. Your guidance will help them conform to the United States' broader cybersecurity strategy and holistically evaluate the net effects on national security. Furthermore, your involvement will help resolve the uncertainty facing businesses as they await resolution of what has already been an overlong process.

We thank you for your leadership on this issue, and we look forward to working with you to support our nation's cybersecurity.

Sincerely,