February 18, 2016

The Honorable John F. Kerry
Secretary
Department of State
Washington, D.C. 20520

The Honorable Penny Pritzker
Secretary
Department of Commerce
Washington, D.C. 20230

The Honorable Jeh Johnson
Secretary
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Kerry, Secretary Johnson and Secretary Pritzker:

Our organizations, representing several of the largest sectors of the U.S. economy, write concerning the Administration's ongoing efforts with respect to the implementation of the Wassenaar Arrangement "intrusion software" and surveillance technology provisions agreed to at the 2013 Plenary. Cybersecurity is not only a top policy priority for our members, but is also fundamental to their continued international competitiveness. While we agree with the laudable goals of the Wassenaar Arrangement, we write today to emphasize the broad range of industries whose cybersecurity efforts would be undermined by the implementation of these provisions in the United States and abroad. Given the cross-border nature of cyber threats, we urge you to pursue a renegotiation of the 2013 Plenary provisions to avoid interference with global cybersecurity efforts.

As recent headlines make clear, our public and private sector networks are under a constant state of attack from sophisticated adversaries who leverage cutting-edge technologies to perpetrate criminal acts. To defend against these threats, network operators in every industry require the most advanced cybersecurity technologies as well as real-time access to vulnerability and other cybersecurity information. The ability to access and harness the global cybersecurity community – including

researchers and academics across the world – is vital to address the ever-evolving threats. The Bureau of Industry and Security's initial proposed rule for implementing the "intrusion software" provisions agreed to at the 2013 Plenary would have substantially undermined the ability of U.S. companies, and indeed global companies, to prevent, detect and remediate cybersecurity incidents in a time-sensitive manner. Based on these concerns, the U.S. Department of Commerce rescinded the proposed rule and committed to working with stakeholders to develop a revised draft rule.

Ultimately, however, the national security risks posed by the "intrusion software" provisions agreed to at the 2013 Plenary cannot be effectively addressed through U.S. policy alone. Because cybersecurity efforts depend on global action, including rapid information sharing among an international community of professionals, it is essential for the United States to take a leadership role in pushing for a renegotiation of these provisions at the Wassenaar Arrangement itself. Unless the Wassenaar Arrangement's approach to controlling "intrusion software" and associated research, development, and information sharing are addressed, multinational companies with cybersecurity teams spread across multiple countries that are members of the Wassenaar Arrangement will find themselves unable to test their own networks, share mission-critical technical information, or deploy the most advanced cybersecurity technologies in a timely and useful manner without first obtaining multiple export licenses. In the United States, the timeline for license application and approval could create significant delays and prevent real-time responsiveness to threats. The troubling trend of erecting barriers to cross-border data flows will only impede cooperative cybersecurity efforts. The impact would also be felt by small- and medium-sized enterprises whose cybersecurity needs are often filled by vendors that also depend upon the free exchange of threat indicators and vulnerability information.

For these reasons, we strongly urge the Department of State to add renegotiation of the 2013 Plenary provisions regarding intrusion software and surveillance technology to the agenda for the 2016 March meeting. The core Wassenaar Arrangement language should be revised with broad consensus from industry, researchers, and other cybersecurity stakeholders. In addition, while we appreciate the Administration's commitment that it will not move forward with a final rule without additional public consultation, we strongly urge you to forego any further rulemaking activity until renegotiation of the 2013 Plenary provisions is complete. Our organizations and member companies stand ready to assist you in achieving these goals.

Sincerely,

American Petroleum Institute (API)
Auto Alliance
BSA | The Software Alliance
Coalition for Responsible Cybersecurity
Computer and Communications Industry Association (CCIA)
Financial Services Roundtable/BITS
Information Technology Industry Council (ITI)
Internet Association
National Association of Manufacturers (NAM)
National Foreign Trade Council (NFTC)
Software & Information Industry Association (SIIA)
TechNet
U.S. Chamber of Commerce