Cybersecurity Coalition

The Cybersecurity Coalition ("The Coalition") is composed of leading companies with a specialty in cybersecurity products and services. We are dedicated to achieving and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies and best practices. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management.

The Coalition submits these comments in response to the Bureau of Industry and Security's ("BIS") interim final rule request for comments regarding *Information Security Controls: Cybersecurity Items*. The Coalition appreciates the opportunity to comment on the proposed export controls pertaining to cybersecurity items, revised Commerce Control List implementation, and the new License Exception Authorized Cybersecurity Exports ("ACE exception").

The Coalition would first like to thank BIS for listening and responding to the Coalition and other industry input on past iterations of the controls for emerging technologies and cybersecurity items as related to the Wassenaar Arrangement ("WA"). The changes made in 2017 to the WA controls are helpful to continue enabling cybersecurity companies and professionals to prevent and respond to cybersecurity threats and incidents, disclose vulnerabilities in a timely manner, conduct threat research, and undertake other beneficial cybersecurity activities. The changes from the BIS 2015 rule, that are now reflected in this 2021 interim final rule, will help U.S. companies to continue to be leaders in the space. The creation of the ACE exception, that authorizes exports of cybersecurity items to many destinations except in certain conditions, may help to address many of the concerns previously expressed by the Coalition. The Coalition would also like to thank BIS for proactively releasing a FAQs document on cybersecurity items and Export Administration Regulations. This document is helpful in clarifying some of the Coalition's initial questions on topics such as the coverage of exploits, software running on servers, and services in the interim final rule.

The interim final rule is highly complex, however, and uses a number of vague terms, many of which are directly incorporated from the WA control language. This makes the rule difficult to comment on, and even more difficult to implement – especially for members of the security community without access to highly specialized export control expertise. Whereas the WA aims to include over 40 member countries, the U.S. is a clear leader in the security community. BIS has an opportunity to take the lead in setting clear guidelines for the U.S. and by extension for the other WA members. Accordingly, we respectfully request that BIS:

1) Develop clear guidelines that answer the questions outlined below;
2) Ensure appropriate opportunities for industry engagement and input on the guidelines; and
3) Delay implementation until the guideline production and subsequent engagement with industry have taken place.

To provide more details on the Coalition's recommendations, we encourage BIS to undertake educational efforts such as meeting with industry and hosting workshops as part of the industry engagement before the interim final rule enters into effect. Furthermore, while producing any guidelines, it is important to ensure the terms "cyber incident response" and "vulnerability disclosure" are defined broadly enough to include all activities needed for effective vulnerability handling, remediation development and cyber incident response, including actions beyond information exchange.

This engagement and guidance should focus on how the new controls related to cybersecurity and the ACE exception would function in practice for exporters. The ACE exception is very complex and includes many exceptions to exceptions. A rule this difficult to write and convey could lead to different interpretations and make it difficult for industry to follow the correct meaning of the rule. Issues that require further clarification include:

a. What specific categories of cybersecurity products do the new controls cover? The Coalition recognizes that the controls included in the interim final rule mirror the WA, but this is the first time these controls would be applied to exports from the United States. Further guidelines would be helpful to ensure that cybersecurity companies are correctly interpreting any nuances that exist between the different controls. The FAQ does address many of the Coalition's questions regarding the coverage of penetration testing software but does not clearly state which other product categories are covered.

b. Could cybersecurity incident detection and monitoring software be covered under *5A001.j*? A core component of organizational security programs, often required by regulation, is the capability to monitor networks for anomalies indicative of a cybersecurity attack or breach. Such software employed for this purpose may be capable of extracting metadata and content (for example, to identify malicious code), as well as some mapping of individual network users (for example, to identify potential impersonators using stolen credentials), as described in *5A001.j.1-2*. Most incident detection and monitoring software does not, however, perform these functions at a national scale. Does *"performing all of the following on a carrier class IP network,"* as that phrase is used in *5A001.j1*, include software operating on any part of a carrier's IP network, or operating on the entire national grade network at once? Furthermore, how will BIS define "carrier class network?"

c. How should exporters navigate the *"reason to know"* standard in ACE when it comes to exporting cybersecurity items to *"favorable treatment cybersecurity end users"* in higher risk *D:1* and *D:5* countries? Several such countries have unclear separation between the government and private sector, as well as questionable intellectual property and human rights records. How does BIS determine whether misuse of an export is *"substantially certain to occur"* without positive knowledge that the recipient intends to misuse the export?

d. Building upon the previous point, regarding the application of favorable treatment cybersecurity end user compared to government end user, the distinction could be unclear in some situations. In some countries, favorable treatment cybersecurity end users (such

as civil health and medical institutions) may provide public services and may receive funding from the government. A BIS clarification to address this unclarity is recommended – in line with the action BIS took to clarify the export of encryption items.

To reiterate, the Coalition appreciates the efforts BIS made in the last few years to engage with and listen to industry when drafting this interim final rule. We believe with further engagement between BIS and industry will only lead to greater success in implementation of the final rule. The Coalition appreciates the opportunity to comment on this important issue and looks forward to continued collaboration with the BIS.