Comments of

TechFreedom

Berin Szoka, President

Mark Potkewitz, Summer Fellow

In the Matter of

Department of Commerce, Bureau of Industry and Security

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items
(Proposed Rule with request for comments)

Docket No. 150304218–5218–01

July 20th, 2015

The Bureau of Industry and Security's (BIS) "Proposed Rule" seeks comments on the implementation of the Wassenaar Arrangement which would add a license requirement to selected "cybersecurity items."[1] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement"), a multilateral export control regime, aims to increase international and regional stability by restricting exports of certain munitions and goods along nine main categories with two annexes delineating *sensitive* and *very sensitive* items.

In principle, we support BIS's effort to minimize the export of U.S. technologies to regimes that will use them against their own citizens. Yet we also recognize that these technologies are necessary for those citizens to defend themselves — and that controlling the transfer of cybersecurity technologies will necessarily burden defense as well as offense, circumvention as well as censorship.

Thus, we were heartened that the Proposed Rule includes the following refreshingly candid admission:

> The impact of this rule is unknown to BIS, therefore the implementation of the Wassenaar Arrangement agreement of 2013 with regard to cybersecurity items is issued as a proposed rule with request for comments concerning the impact of the rule.

If only more regulators were so willing to admit "how little they really know about what they imagine they can design" — to use the most famous line from *The Fatal Conceit*, F.A. Hayek's 1988 magnum opus about the perils of top-down planning.[2] Illustrating this, as Hayek argued, is "the curious task of economics": to probe the likely consequences, as far as can be foreseen, of any possible regulation. It is also what BIS must do if it is to balance liberty with security in the broadest sense.

In this case, the costs and benefits of restraining the flow of cybersecurity technologies are both economic, in the traditional sense of financial costs for companies and effects on markets, and "non-economic," in the broader sense of costs that are more difficult to quantify in financial terms. Among the trade-offs that must be considered are:

- Will U.S.-based cybersecurity firms move overseas?
- Will foreign-based cybersecurity firms be reluctant to do business with U.S. customers and firms?
- Will new rules make it more difficult for foreign system operators, both private and public, and individuals to defend themselves from attack?
- Will new rules undermine cybersecurity research?
- Will new rules hamper collaborative efforts between international security experts?
- Will new rules prevent firms with international offices from using the same tools across offices?
- How will new rules affect cybersecurity startups, in particular?

---

[1] Department of Commerce Bureau of Industry and Security, 80 Fed. Reg. 97 (May 20, 2015), available at http://www.bis.doc.gov/index.php/forms-documents/doc_download/1236-80-fr-28853 .

[2] Friedrich Hayek, *The Fatal Conceit: The Errors of Socialism* 76 (1988).

Whether BIS is legally *required* to engage in any form of cost-benefit analysis is irrelevant to whether it *should* do so. Indeed, Executive Order 13563 — which the Proposed Rule specifically cites, without any further commentary — makes no exception for national security related matters. It requires that, in general,

> **each agency must**, among other things: (1) propose or adopt a regulation only upon a **reasoned determination** that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (2) **tailor its regulations** to impose the **least burden** on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the **costs of cumulative regulations**; (3) select, in choosing among alternative regulatory approaches, those approaches that **maximize net benefits** (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity); (4) to the extent feasible, specify **performance objectives**, rather than specifying the behavior or manner of compliance that regulated entities must adopt; and (5) identify and assess **available alternatives** to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public.[3]

This is the "gold standard" to which BIS should aspire. Doing so requires soliciting comments on potential costs and benefits, precisely as BIS has done in the Proposed Rule — but also that BIS issue a report on its analysis along with any modifications to the Proposed Rule that may be required by that analysis *before* issuing a final rule. Jumping straight to a final rule without giving the public an additional opportunity to comment on both BIS's cost-benefit analysis and the revised rules would render any cost-benefit analysis the agency might perform essentially perfunctory: only further public comment can ensure that this analysis is adequately rigorous and that BIS further revise its rules as necessary.

Cybersecurity is simply too important for BIS to rush this rulemaking. We look forward to providing additional comment on BIS's revised rules — and to seeing BIS's report on the costs and benefits of its proposal.

[3] Exec. Order No. 13563, 76 C.F.R. 14 (2011) (emphasis added).