ELECTRONIC FRONTIER FOUNDATION eff.org

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave. NW.
Washington, DC 20230

VIA Email: publiccomments@bis.doc.gov

RE: Comments of the Electronic Frontier Foundation on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694-AG49

To Whom it May Concern:

The Electronic Frontier Foundation (EFF) submits the following comments to the Bureau of Industry and Security (BIS) in response to the Proposed Rule and Request for Comments on the Wassenaar Arrangement (WA) 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694-AG49, dated May 20 2015 (Proposed Rule). In addition to these comments, EFF joins in full the comments submitted by the group of civil society organizations consisting of Access, Center for Democracy and Technology, Collin Anderson, EFF, Human Rights Watch, and New America's Open Technology Institute (Joint Comments). We submit these brief comments to supplement and expand on our more complete joint civil society submission.

We urge BIS to revise the Proposed Rule and open another public Request for Comments on the revision. As part of that process, we urge BIS to take what it learns as part of this rulemaking to the greater international export control community in December 2015 at the next annual meeting of the WA members, and work with them to improve the text of the WA control lists directly.

BIS is familiar with the Wassenaar Arrangement and the 2013 additions to the WA control lists so we will not summarize them or their history here. Similarly, because EFF is a legal organization and not a software vendor, we will not focus on specific products here, except when necessary. We understand that several knowledgeable companies and trade organizations will be submitting comments to this Proposed Rule and we trust them to give specific examples of how the Proposed Rule will impact their businesses directly. These comments are instead intended to give an overview of what we think some major issues with the Proposed Rule are, and some ways in which BIS might address them.

These comments are limited to the addition of intrusion software controls in ECCN 4A005 and related amendments to ECCN 4D001, ECCN 4E001, and § 740.13; we do not address the Proposed Rule as it applies to ECCN 5A001.j regarding Internet Protocol (IP) Network Communications Surveillance Systems.

1. About the Electronic Frontier Foundation

EFF is a nonprofit, member-supported civil liberties organization working to protect privacy and free expression in technology, law, policy, and standards in the information society. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With

over 21,000 dues-paying members and over 284,000 mailing-list subscribers, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

EFF has been a leading voice defending the rights of security researchers since the 1990s when we represented Professor Daniel J. Bernstein in his successful challenge to the inclusion of open source cryptography in the International Traffic in Arms Regulations (ITAR). We believe that the Proposed Rule is too vague to be feasible, technically flawed, and almost certainly unconstitutional.

2. Specific Concerns and Recommendations

- Eliminate Encryption Items from the EAR

Strong cryptography is a necessary and daily part of our lives in the digital era. The freedom to use encryption technology is often a prerequisite for everything from online commerce to the exercise of the rights of privacy and expression, that it can no longer be rationally thought of as a dual-use technology. As it notes in the preamble, many of the technologies the Proposed Rule would control "are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality" and therefore the rule would add little additional burden. Much of the work of the Proposed Rule seems to hinge on that assumption and much of BIS' response to questions about the scope of the Proposed Rule refer to the fact that intrusion software is often already controlled if it contains encryption or cryptanalytic

functionality. However, cryptography is a core component of everything from web browsers,[1] to mobile phones,[2] to music players[3] and as such, does not reasonably belong in the EAR.

Both individuals and government agencies rely on strong encryption in their daily activities. Moreover, human rights activists, journalists, refugees, bloggers, and whistleblowers rely on strong encryption technologies to protect their communications, the names and location of their sources and/or witnesses, etc. Even the relatively hands-off control of encryption in the EAR impacts freedom of expression in two ways. First and foremost, it makes it harder for small developers to publish their work. Second, any attempt to restrict the distribution of encryption technologies that did not follow the EAR's process would impact the rights of software creators to express their viewpoint through code. Furthermore, many security researchers provide open-source encryption software and disclose algorithms as an integral part of examining the encryption technology for flaws and weakness. This means that the encryption technology purportedly controlled by the EAR is already freely available throughout the world. It is time for the EAR to be updated to reflect the fact that encryption is a civilian technology that is critical to protecting our democracy, our right to free expression, and our security.

The encryption controls should be removed from Category 5 part 2 of the EAR as part of any revision to the Proposed Rule. The controls on Encryption Items function only to impose a bureaucratic headache on American businesses and developers without any benefit to commerce or national security.

[1] http://research.google.com/pubs/SecurityCryptographyandPrivacy.html
[2] https://www.apple.com/business/docs/iOS_Security_Guide.pdf
[3] https://sonos.custhelp.com/app/answers/detail/a_id/2638/~/sonos-wifi-setup

- BIS Should Revise the Proposed Rule and Open a New Request for Comments

EFF is confident that BIS will revise the Proposed Rule in response to the comments it receives in this rulemaking. However, in order to avoid the technical ambiguity that plagues this Proposed Rule, the revision process must be iterative and collaborative. Even though it will unavoidably introduce delay into the process, BIS should issue a revised Proposed Rule and reopen a public Request for Comments on the revisions to the Proposed Rule after consulting with industry, academia, and civil society.

Further, BIS cannot and does not operate in a vacuum. Much of the technically problematic language from the Proposed Rule (e.g., defining "intrusion software" as software that performs a "modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions") comes directly from the WA. As such, we urge BIS to work within the WA at the December 2015 annual meeting to ensure that changes to the definitions are integrated upstream into the WA control lists themselves. We urge BIS to wait until after that process is complete before issuing a revised Proposed Rule and Request for Comments.

- BIS Should Clarify What it Intends to Control

For years, there's been ample evidence that authoritarian governments around the world are relying on the technology of U.S. and European companies to facilitate abuse of human rights, with a wealth of recent evidence in the Arab Spring and China. But in the Preamble to the Proposed Rule, BIS does not actually state its goal for this rule, but instead parrots the control lists' definitions.

That lack of clarity has left the public having to guess what BIS' aims are and which types of technologies BIS intends to regulate. Some of that confusion is inherent in the WA language itself, but much of it comes from a lack of clear limiting statement from BIS. And as BIS has seen over the last two months, there has been an overwhelming need for clarification of the rules.[4]

As it revises the Proposed Rule, we urge BIS to also revise the Preamble to present a clear statement on the *intended* scope of the regulation. Simply repeating the technical language from the control lists caused more confusion than it resolved. Does BIS intend to control only those systems that are specially designed for use by governments? If so, BIS should clearly so state.

From the perspective of academics, security researchers, and open-source developers, it would be better to be faced with a clearly-worded, clearly-defined rule that the community did not necessarily agree with, than a difficult to understand rule that seemed to implement policies that the community would support, if only it could only understand what the rule meant. To give a specific example, in FAQ #4,[5] BIS stated that the Proposed Rule would control "information 'required for' developing, testing, refining, and evaluating 'intrusion software', in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information." It is clear to EFF that BIS does not intend to control penetration testing frameworks or debuggers, but from the answer to the FAQ above, that intent is not effectively conveyed.

[4] *See, e.g.*, the fact that a 32-question FAQ was necessary. https://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200
[5] *Id.*

The vagueness of the WA control lists has real world chilling effects on fundamental academic research. Take for example the dissertation of a student at the University of Northumbria named Grant Wilcox.[6] EFF does not believe that censorship of Mr. Wilcox's paper required by the WA control lists. However, the fact of the matter is that Mr. Wilcox's university ethics board did censor the dissertation, believing it to be possibly within the WA definitions. This instance is only one recent and particularly clear example among many of the unintended chilling effects of vaguely worded regulation. From an EFF perspective, examples such as the needless censorship of Mr. Wilcox's dissertation strongly caution against proceeding with an implementation of the WA in the United States without first clarifying the scope of what exactly the rules are intended to control.

- Potential Constitutional Problems with the Proposed Rule

EFF understands that BIS is seeking information about the effect of the Proposed Rule specifically as applied to industry and is not inviting legal arguments. However, the nature of EFF compels us to point out two potential constitutional problems with the Proposed Rule that would likely cause a court to invalidate the rule if it went into effect as currently drafted, or at best tie it up in litigation for years before it went into effect.

First, the Proposed Rule would act as an unconstitutional prior restraint on speech in violation of the First Amendment. In 1999, a U.S. Court of Appeal agreed with EFF that a broad range of individual rights were implicated by government controls on the discussion of source code:

> [W]e note that the government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment

[6] http://tekwizz123.blogspot.com/2015/07/final-year-dissertation-paper-release.html

> rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, see *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 115 S.Ct. 1511, 1524, 131 L.Ed.2d 426 (1995), the right against compelled speech, see *Wooley v. Maynard*, 430 U.S. 705, 714, 97 S.Ct. 1428, 51 L.Ed.2d 752 (1977), and the right to informational privacy, see *Whalen v. Roe*, 429 U.S. 589, 599-600, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977).

Bernstein v. United States Dept. of Justice, 176 F.3d 1132, 1145-46 (9th Cir. 1999). While the Ninth Circuit in *Bernstein* was discussing the encryption rather than the cybersecurity items controlled by the Proposed Rule, much of the reasoning is similarly applicable. By failing to adequately consider the technology, information, and tools necessary for industry professionals to protect the digital security we all depend on,[7] the Proposed Rule implicates more than just the rights of security software vendors. Any attempt to slow or stop the advancement of the state of the art of computer security through control under the EAR will be subject to the highest level of constitutional scrutiny. A narrowly-cabined rule, one limited to controls of end uses or end users,

[7] *See e.g.,* Comment of Cisco Systems, Inc. https://blogs.cisco.com/wp-content/uploads/Cisco_Wassenaar_Final_07202015.pdf

as we recommend in the Joint Comments would be much more likely to stand up if challenged in court.

Second, if regulations that carry criminal penalties (as the EAR does, *see* 15 C.F.R. § 764.3(b)), those regulations "are impermissibly vague [if] they fail to give notice of the conduct they regulate and have a chilling effect on speech."[8] Only if the definition of prohibited conduct as well as "the exemptions from this definition are clear to a person of ordinary intelligence" may a criminal penalty pass constitutional muster.[9] As worded, the Proposed Rule and its exemptions are not clear to a person of ordinary intelligence. BIS' own FAQ in response to the Proposed Rule is ample demonstration that persons of much greater than ordinary intelligence are confused by the Proposed Rule. Therefore unless BIS revises the Proposed Rule to the point where it is "clear to a person of ordinary intelligence"—not an industry insider, an export control lawyer, or the rare software developer versed in parsing statutory language—a court would be likely to strike down the rule as unconstitutionally vague.

3. Conclusion

EFF respectfully urges BIS to carefully consider the quality and quantity of the comments it receives in opposition to the current Proposed Rule. In addition to the comments submitted by the group of civil society organizations consisting of Access, Center for Democracy and Technology, Collin Anderson, EFF, Human Rights Watch, and New America's Open Technology Institute, we urge BIS to (1) eliminate all controls on cryptography from the EAR before proceeding with implementing the Wassenaar Arrangement 2013 Plenary Agreement, (2)

[8] *Bernstein v. US Dept. of State*, 922 F. Supp. 1426, 1439 (N.D. Cal. 1996).
[9] *Id.*

revise the Proposed Rule and reopen a second public comment period, and (3) carefully consider the Due Process and First Amendment implications of any vaguely-worded prior restraint of the dissemination of knowledge.

Sincerely

Nate Cardozo
Staff Attorney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94611