Comments to the U.S. Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements

(RIN 0694-AG49)

July 20th, 2015

Submitted by

Access,
Center for Democracy & Technology,
Collin Anderson,
Electronic Frontier Foundation,
Human Rights Watch &
New America's Open Technology Institute[1]

Access, the Center for Democracy & Technology, Collin Anderson, the Electronic Frontier Foundation, Human Rights Watch, and New America's Open Technology Institute respectfully submit these comments to the U.S. Department of Commerce in response to the Bureau of Industry and Security's Request for Comments on Wassenaar Arrangement 2013 Plenary Agreements Implementation.[2]

Access is an international, non-profit organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

The Center for Democracy & Technology (CDT) is a nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communication technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways.

Collin Anderson is a Washington, D.C.-based computer scientist focused on Internet controls and restrictions on communications, including network

[1] Contact Laura Moy, Senior Policy Counsel, Open Technology Institute, moy@newamerica.org.

[2] Bureau of Industry and Security, "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items," *Federal Register* Vol. 80 No. 97, May 20, 2015, https://federalregister.gov/a/2015-11642 (80 FR 28853).

ownership, disruption of access and regulatory regimes, with an emphasis on countries that limit the free flow of information.

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.

Human Rights Watch (HRW) is an independent global organization that monitors human rights in more than 90 countries around the world. HRW defends the rights of people worldwide by scrupulously investigating abuses, exposing the facts widely, and pressuring those with power to respect rights and secure justice.

New America is a nonprofit, nonpartisan public policy institute based in Washington, D.C. that invests in new thinkers and new ideas to address the next generation of challenges facing the United States and the global community. The Open Technology Institute is a program within New America that promotes affordable, universal access to open and unrestricted communications networks through technology development, applied learning, and policy reform.

I. Introduction

We sincerely thank the Bureau of Industry and Security (BIS) of the Department of Commerce for taking the time to solicit public comments on the proper implementation of the 2013 Wassenaar controls related to Intrusion and IP Network Surveillance Items. We hope the opportunity for public comment helps BIS to better understand how the proposal will impact the information and communications technology market and related technical communities.

The organizations that we represent are familiar not only with the technical elements of the proposed rule, but also with the human rights concerns that led the French and UK governments to propose the original controls in 2013. The goal of our comments is both to provide specific information about aspects of the rule that are either ambiguous or otherwise concerning, and to offer concrete recommendations to address these problems. We believe it is possible for Commerce to craft a final rule that is narrowly tailored to address the human rights concerns raised by the spread of the single-use surveillance technologies without adversely affecting a variety of additional technologies, including important security research and testing tools.

These comments are structured as follows:

- **Part II** describes the policy challenge that the original Wassenaar controls related to Intrusion Software and IP Network Surveillance Systems sought to control and the wide range of evidence that has emerged in recent years about the human rights abuses that are facilitated by the export of these technologies to repressive regimes;

- **Part III** describes the original scope and intent of the surveillance-related controls adopted by the members of the Wassenaar Arrangement at the 2013 Plenary meeting;

- **Part IV** offers a number of recommendations for how BIS can tailor its approach to address concerns about overbreadth without sacrificing the important policy goal of addressing the human rights abuses facilitated by the export of these technologies, including:

    - Apply the Technology and Software – Unrestricted (TSU) license exception to cybersecurity software.
    - Issue broad license authorizations for transfers of penetration testing software and hardware that does not qualify for license exceptions to non-governmental use and users.
    - After adopting license exception TSU and broad license authorizations for non-governmental use and users, tailor the licensing process for remaining items specifically to human rights concerns regarding cybersecurity items.
    - Provide guidance on the "generation" component of ECCN 4D004 to decontrol certain classes of development tools.
    - Narrow the control on technology for the "development" of Intrusion Software so that it only applies to transfers to government end users or for military or law enforcement purposes.
    - Provide clear "Know Your Customer" guidance.
    - Issue clear guidance on key terminology introduced into the text of the rule.
    - Establish a transparent and iterative process to assess the success of the rule after it has been applied and adjust it as necessary to address possible over- or under-breadth.

II. The Policy Challenge: Human Rights Abuses Facilitated by the Export of Surveillance Technology to Repressive Regimes

The uncontrolled export of surveillance technologies to countries with dubious human rights records poses a growing, significant threat to fundamental rights and the free flow of information online.[3] These tools – commonly marketed directly to governments and designed to build surveillance and privacy-invasion capabilities into a country's communications infrastructure – not only undermine the work of human rights groups and journalists to hold governments democratically accountable, but also endanger the daily lives of individual citizens. After the revolutions that swept the Arab world in 2011, archives obtained from those fallen regimes showed that a number of Western companies had been supplying censorship and surveillance technology to these and other repressive governments despite their poor human rights records.[4] These revelations have subsequently been supported by extensive research from a variety of academic institutions and human rights organizations, including the University of Toronto's Citizen Lab, Reporters Without Borders, Access, Human Rights Watch, and Privacy International.[5] Recently-leaked documents describing the operations of Hacking

[3] These fundamental rights include, *inter alia*, the right to privacy and the right to freedom of expression, which are affirmed and protected by the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR), which the U.S. has ratified. Recent interpretations of these rights are found in: Human Rights Committee, "General Comment 34," 2011, http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf; Navi Pillay, UN High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; reports by Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, and 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf; and his successor Special Rapporteur David Kaye, in 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

[4] See, e.g., Karen McVeigh, "British firm offered spying software to Egyptian regime – documents," *The Guardian*, April 28, 2011, http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher; Paul Sonne & Margaret Coker, "Firms Aided Libyan Spies," *The Wall Street Journal*, August 30, 2011, http://www.wsj.com/news/articles/SB10001424053111904199404576538721260166388; "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," *Bloomberg Business*, November 3, 2011, http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear; Vernon Silver, "Hewlett Packard Computers Underpin Syria Surveillance Project," *Bloomberg Business*, November 18, 2011, http://www.bloomberg.com/news/articles/2011-11-18/hewlett-packard-computers-underpin-syria-electonic-surveillance-project; Trevor Timm & Jillian C. York, "Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators," *The Atlantic*, March 6, 2012, http://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/.

[5] See, e.g., Morgan Marquis-Boire, et al., "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," *The Citizen Lab*, January 15, 2013, https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/; Morgan Marquis-Boire, et al., "Some Devices Wander By Mistake: Planet Blue Coat Redux," *The Citizen Lab*, July 9, 2013, https://citizenlab.org/2013/07/planet-blue-coat-redux/; "The Enemies of the Internet: Corporate Enemies," *Reporters Without Borders*, March 2013, https://surveillance.rsf.org/en/category/corporate-enemies/; "Commonwealth of Surveillance States," *Access*, June 2013, https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046_8sm6ivg69.pdf; "Ethiopia: Telecom Surveillance Chills Rights: Foreign Technology Used To Spy on Opposition Inside the Country, Abroad," *Human Rights Watch*, March 25, 2014, https://www.hrw.org/news/2014/03/25/ethiopia-

Team, an Italian vendor of Intrusion Software, provide further evidence of the proliferation of Western surveillance technologies to repressive countries, with notable clients such as Azerbaijan, Bahrain, Ethiopia, Kazakhstan, Nigeria, Oman, Saudi Arabia, and Uzbekistan, as well as sanctioned states like Sudan and Russia.[6]

As this evidence has emerged in the past few years, human rights advocates and policymakers have explored various ways to hold accountable American and European companies that develop and sell these products when they facilitate human rights abuses. Some businesses in the United States, United Kingdom, and France have faced legal challenges for violating human rights under existing domestic laws.[7] While these efforts have generated significant media attention, their efficacy as a legal strategy to actually provide redress against the companies selling these technologies – particularly in the U.S. – has been less clear. Consequently, another proposal that has gained some support is to use export controls to curb the unfettered proliferation of such technologies to countries with dubious human rights records and give the government a clear path to penalize the companies that violate these regulations.[8] Making a narrow and specific group of technologies subject to a licensing regime for review prior to export – based on their technical characteristics as well as their destination and likely end-use – is one potential avenue to address important human rights concerns created by the proliferation of monitoring and censorship technology.[9]

telecom-surveillance-chills-rights; "Private Interests: Monitoring Central Asia," *Privacy International*, November 2014, https://www.privacyinternational.org/?q=node/293.

[6] *See*, *e.g.*, Sarah Myers West, "Hacking Team Leaks Reveal Spyware Industry's Growth, Negligence of Human Rights," *Electronic Frontier Foundation*, July 8, 2015, https://www.eff.org/deeplinks/2015/07/hacking-team-leaks-reveal-spyware-industrys-growth; Joshua Kopstein, "Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech," *Motherboard*, July 6, 2015, http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech.

[7] In 2012, the French government opened up a judicial inquiry against Amesys, a division of the French company Bull, to look into its operations in Libya after two human rights groups filed formal complaints about the alleged sale of surveillance systems to the Qaddafi regime. Ryan Gallagher, "French Company That Sold Spy Tech to Libya Faces Judicial Inquiry Amid New Allegations," *Slate*, June 19, 2012, http://www.slate.com/blogs/future_tense/2012/06/19/amesys_facing_inquiry_in_france_over_selling_eagle_surveillance_technology_to_qaddafi_.html; for more details on the formal complaint, see "Opening of a judicial inquiry targeting Amesys for complicity in acts of torture in Libya," *FIDH*, May 24, 2012, https://www.fidh.org/International-Federation-for-Human-Rights/north-africa-middle-east/libya/Opening-of-a-judicial-inquiry. In the United States, Cisco has been sued for selling equipment to the Chinese government that was used as part of its censorship and surveillance regime. Rainey Reitman, "Cisco and Abuses of Human Rights in China: Part 1," *Electronic Frontier Foundation*, August 22, 2011, https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1.

[8] Danielle Kehl & Tim Maurer, "Against Hypocrisy: Updating Export Controls for the Digital Age," *CyberDialogue*, March 9, 2013, http://www.cyberdialogue.ca/2013/03/against-hypocrisy-updating-export-controls-for-the-digital-age-by-danielle-kehl-and-tim-maurer/.

[9] For an in-depth discussion, see Tim Maurer, Edin Omanovich, and Ben Wagner, "Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age," *New America's Open Technology Institute*, *Privacy International & Digitale Gesellschaft*, March 2014, http://www.newamerica.org/oti/uncontrolled-global-surveillance-updating-export-controls-to-the-digital-age/.

The idea of using trade restrictions to address human rights concerns related to communications technologies is not without precedent in the United States. Indeed, the U.S. exercises broad sanctions against particular countries for human rights abuses. Since 2010, the U.S. government has maintained additional prohibitions on exporting "sensitive technology" to Iran, which includes hardware, software, and telecommunications equipment that can be used "to restrict the free flow of unbiased information" or "disrupt, monitor or otherwise restrict speech."[10] The sensitive technologies language represents an acknowledgement by the U.S. government that surveillance and censorship technologies are often abused by repressive regimes, and that penalties for companies caught exporting such tools should be severe. In 2012, the United States also began restricting the export of IMSI catchers – devices that enable "man in the middle attacks" and intercept mobile phone traffic by impersonating cell phone towers – after similar language was adopted by the Wassenaar Plenary.[11]

This approach is not without risks, however. There has long been apprehension about export controls among those in the technical community who remember the "Crypto Wars" of the 1990s: an infamous battle over the broad and messy restrictions placed on cryptography exports.[12] Although the United States has relaxed most limits on the export of encryption since 1999, further liberalization of encryption controls is still required and similar concerns about complexity and the risk of overreach with export controls should not be overlooked. The language used to describe the scope of the systems being controlled needs to be flexible enough to catch the targeted products, while at the same time specific enough to ensure that other tools and services are not inadvertently covered.[13] Achieving this delicate balance is critically important for security researchers and professionals, especially since it can be challenging to differentiate between defensive products used to protect systems and those that are used to compromise them.

Export controls are not a panacea and their application will neither eliminate the trade in censorship and surveillance technologies, nor mitigate threats posed by

[10] Christopher M. Matthews, "State Department Clarifies 'Sensitive Technologies' Sanctions," *The Wall Street Journal*, November 13, 2012, http://blogs.wsj.com/corruption-currents/2012/11/13/state-department-clarifies-sensitive-technology-sanctions/.

[11] Jamie Doward & Rebecca Lewis, "UK 'exporting surveillance technology to repressive nations," *The Guardian*, April 7, 2012, http://www.theguardian.com/world/2012/apr/07/surveillance-technology-repressive-regimes; *Federal Register* Vol. 77 No. 127, July 2, 2012, http://www.bis.doc.gov/index.php/forms-documents/doc_view/577-77-fr-39353 (describing changes to Category 5, Part 1 – Telecommunications).

[12] For an in-depth discussion of the history of U.S. export controls on cryptography, *see* Section III, "The Battle Over Encryption Export Controls," in Danielle Kehl, Andi Wilson & Kevin Bankston, "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," *New America's Open Technology Institute*, June 2015, http://www.newamerica.org/oti/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/.

[13] Edin Omanovich, "Export Controls and the Implications for Security Research Tools," *Privacy International*, December 8, 2013, https://privacyinternational.org/?q=node/354.

producers of such systems located in countries not subject to the Wassenaar Arrangement. Surveillance technologies produced within countries that are members of the Wassenaar Arrangement, however, are often more sophisticated than the other systems available in the international marketplace and therefore warrant additional scrutiny. Properly-implemented export controls can be a valuable tool to help curb the unregulated spread of these systems and promote broader norms, which is important not only given the United States' role in the international sale of Intrusion Software and IP Network surveillance technologies, but also its leadership in promoting Internet Freedom and responsible business and human rights practices. Even when they are not invoked to restrict a transfer of surveillance technology, export controls also act as an essential accountability and transparency mechanism. Greater transparency into this industry can assist the U.S. government in monitoring the human rights impact of U.S. businesses and improving policies to address abuses and enhance remedies where companies cause or contribute to human rights harms.

III. Surveillance-Related Controls Adopted by the Members of the Wassenaar Arrangement at the 2013 Plenary Meeting

At the conclusion of the 2013 Wassenaar Plenary meeting, its members announced that they were adopting new controls relating to "Intrusion Software" and "IP network surveillance systems."[14] "Intrusion Software" is designed to surreptitiously intercept activities and communications on electronic devices, such as passwords, screenshots, microphone recordings, camera snapshots, and Skype chats, and to remotely execute commands. "IP network surveillance systems" constitute mass surveillance platforms – systems to monitor general network traffic for large populations of Internet users in order to identify and collect information about those users. It is clear from the language used in the Wassenaar Plenary Agreements, the motivations of the member states that brought the original proposals, and BIS's justification of the imposition of the National Security control that the intent of the new controls is to restrict the sale of systems that can be used to commit human rights abuses.

When these new controls were announced, a number of human rights organizations supported the decision to control a specific set of single-use surveillance technologies, recognizing the incorporation of human rights considerations into the discussions at a traditionally security-focused forum like

[14] Edin Omanovich, "International Agreement Reached Controling Export of Mass and Intrusive Surveillance Technology," *Privacy International*, December 8, 2013, https://privacyinternational.org/?q=node/398.

the Wassenaar Arrangement as a step forward.[15] A number of academics and civil society organizations also submitted proposed guidance to the agencies responsible for implementing export controls nationally (both in the United States and the European Union), advising them on what to consider when implementing the controls.[16]

At the same time, however, many human rights organizations recognized that there were risks that the proposed controls could be interpreted in an overbroad manner. In addition to urging the relevant agencies to implement the new controls outside of existing encryption controls, these groups placed heavy emphasis on concerns about how the controls associated with Intrusion Software could impact security research if implemented in an overbroad manner. Moreover, these comments stressed the importance of the General Software Note and General Technology Note in preventing a chilling effect on essential security practices and the development of information security tools by exempting open source systems, research, and mass-market security software from these regulations.[17]

For example, recommendations published by Access, Collin Anderson, Internews, Reporters Without Borders, and New America's Open Technology Institute in May 2014 advised U.S. government agencies involved in implementing the controls that:

- "Protecting research and general purpose computing is critical to promoting Internet security, and new controls should be implemented in a manner that aligns with existing technology and software exemptions. We recommend that Wassenaar's 'General Technology Note' and 'General Software note under the Technology and Software – Unrestricted exemption' are replicated explicitly in American regulations for Intrusion Software."[18]

[15] *See*, e.g., "International Body Moving to Restrict Export of Surveillance Systems Used to Commit Human Rights Abuses," *New America's Open Technology Institute*, December 9, 2013, https://www.newamerica.org/oti/international-body-moving-to-restrict-export-of-surveillance-systems-used-to-commit-human-rights-abuses/.

[16] "Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding 'Intrusion Software' and 'IP Network Communications Surveillance Systems,'" Submitted by Access Now, Collin Anderson, Internews, Reporters Without Borders, and New America's Open Technology Institute, May 5, 2014, http://www.newamerica.org/oti/human-rights-and-technology-organizations-submit-joint-recommendations-to-the-us-government-on-the-implementation-of-the-2013-wassenaar-amendments-on-surveillance-technology/ ("Joint Civil Society Recommendations for U.S. Implementation").

[17] *See* Collin Anderson, "Considerations on the Wassenaar Arrangement Control List Additions for Surveillance Technologies," *Access*, March 2015, https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf. In particular, "There is indication that special care was taken to limit potential overreach in the drafting of the Intrusion Software control. For example, the definition attempts to mitigate over-broadness through defining a set of exemptions, as well as not directly controlling Intrusion Software itself. Additionally, while the majority of the Wassenaar Arrangement's Controls for Technology cover the 'development, production, or use' of controlled systems, the Intrusion Software's Technology controls only covers 'development' [4. E. 1. c.]."

[18] Joint Civil Society Recommendations for U.S. Implementation, 3.

- "In contrast to the technical specificity of IP network surveillance, the controls outlined for Intrusion Software could potentially be interpreted broadly... to include more than commercial surveillance technologies. Intrusion controls should not threaten the public's ability to control personal devices or prevent researchers from engaging in security auditing, even where it may include the discovery of vulnerabilities . . . [O]verbroad language could intentionally or inadvertently be used to stifle jailbreaking, security research, and additional activities that would otherwise promote privacy or general purpose computing."[19]

Anticipating the risks of overbreadth, the 2013 Wassenaar Plenary includes several provisions aimed at ensuring that the proposed controls are appropriately tailored in their application, exempting commercial and research technologies. This reflects Wassenaar's goal of controlling the export of technology to nation-state level actors while avoiding interfering with mass-market software and systems. In particular, the agreement includes both the General Technology Note and the General Software Note. These decontrol notes are available to the 2013 Wassenaar "Intrusion Software" categories (4.A.5, 4.D.4, and 4.E.1.c) as well as to the 2013 Wassenaar "Network Surveillance" category (5.A.1.j). Indeed, such exceptions are critical to ensuring that the new categories are not asserted in an overboard manner.[20]

IV. Recommendations for Implementation of the Wassenaar Arrangement 2013 Controls on Intrusion Software

As the Bureau of Industry and Security considers ways to tailor its proposed implementation of the Wassenaar Arrangement 2013 controls to address concerns about overbreadth articulated by security researchers, we offer a number of recommendations to assist with that goal, detailed in this section.

The overarching objectives of our recommendations are to narrow application of the rule only to those circumstances that implicate the human rights and foreign intelligence concerns that provoked the original proposals, to ensure that the licensing policies applied to otherwise inflexible control language strongly protect against the provision of technologies that will contribute to the infringement of fundamental rights, and to reduce the likelihood of adverse effects on security research and practices. The proposals brought by the French and UK governments to the Wassenaar Plenary in 2013 sought to control platforms and technologies

[19] *Id.*, 10.

[20] Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies."

designed to perform the remote compromise of communications devices or mass interception of traffic for the purposes of surveillance.[21] We urge BIS to maintain that focus.

We also believe that the final rule will require further clarification from BIS on the scope and language of the controls, bearing in mind that the current draft rule affects communities (e.g. security researchers and independent software developers) that have not traditionally interacted with the export control system and may need assistance navigating the complexities of the Export Administration Regulations. It is also important to note that many of these individuals and smaller commercial entities may not have the resources to adequately handle the licensing process.

A. "Cybersecurity Software" should be subject to license exception TSU

The 2013 Wassenaar language applies the General Software Note decontrol language to all of the newly proposed 2013 Cybersecurity Items.[22] Traditionally, BIS has implemented the mass-market provisions of the General Software Note via the TSU (Technology and Software - Unrestricted) license exception.[23] However, the proposed implementation of the new categories explicitly excludes the Cybersecurity Items from license exception TSU via proposed sub-section 740.13(d)(2)(ii).[24] BIS asserts that this "cybersecurity software" TSU exclusion is necessary to stay "consistent with the existing encryption exclusion" because "software described in the new control list entries may incorporate encryption functionality."[25] This interpretation, however, risks an overbroad application of the new controlled categories, triggering many of the concerns raised by the security research and practitioner community regarding the proposed rule. Such an

[21] In prior publications, researchers identified a number of vendors of such products, including for Intrusion Software: FinFisher (formerly Gamma Group), Hacking Team, DigiTask, AGLAYA, RCS Lab, Gr Sistemi (Dark Eagle), Clear-Trail Technologies (QuickTrail), Stratign (Spy Phone), SS8 (Interceptor), iPS (ITACA); for IP Network Surveillance: ETI Group's EVIDENT Investigator, SS8 Communications Insight (Intellego), Area SpA MCR Studio, Amesys's EAGLE GLINT (Nexa Technologies SAS), AMECS's Analys, Narus nSystem, Vastech ZEBRA, Group 2000's Lawful Monitoring Centre, Glimmerglass CyberSweep Sapience, ATIS Klarios Monitoring Centre, Siemens Intelligence Platform, Verint Systems, AQSACOM Aqumen, Nice Systems. see *Access*, *supra.*

[22] WA-LIST (13) 1 04-12-2013, 3.

[23] 15 CFR 740.13; Separately, the "public domain", "fundamental research", and related components of the General Software and General Technology Notes are codified via 15 CFR 734.3.b.3.

[24] 80 FR 28853. "§ 740.13–license exception TSU"; While the public domain and fundamental research exemptions remain available to "cybersecurity software" via 734.3.b.3, mass-market software that does not qualify for such exemptions (e.g. because it is not freely available) that would otherwise be eligible for the General Software Note exemption will not be able to take advantage of the TSU exemption under the rules as currently proposed.

[25] 80 FR 28853. "§ 740.13–license exception TSU"; BIS Intrusion and Surveillance Items FAQ #23, available at https://www.bis.doc.gov/index.php/policy-guidance/faqs.

interpretation also fails to reflect existing issues with the restriction on license exception TSU for encryption software.

Furthermore, the proposed TSU exclusion does not align with the intended Wassenaar interpretation or other countries' implementations of the rules. Multi-national control regimes such as Wassenaar are most effective when all involved countries interpret and implement the rules consistently. Since many of the systems the new rules aim to control are manufactured by non-U.S. companies, deviating from the General Software Note by adding additional restrictions to only the U.S. implementation of the rules amounts to a unilateral control, which will do little more than unduly burden U.S. companies and researchers without serving any additional human rights interests.[26]

BIS should therefore apply license exception TSU to the proposed "cybersecurity software" categories.[27] A license exception for mass-market cybersecurity software will help ensure that the new control categories do not adversely affect the distribution of penetration testing tools, network security tools, or other categories of items that may be inadvertently caught by these controls – and will address many of the deemed export and inter-company/university transfer issues that threaten to create an onerous burden on international companies and educational institutions. This conclusion is based on the following considerations:

1. *Mass-market cybersecurity software does not present as substantial a threat to human rights as systems designed for and marketed to state-level actors.*

The Wassenaar Arrangement is designed to control the sale of software to nation-state level actors. To the extent that software is generally available on the mass market, via either the publication of source-code or the provisions outlined under the TSU, it should not be controlled by Wassenaar.

Decontrolling mass-market software will not run contrary to the objectives of the proposed rule. The controls, as originally conceived, were intended to exercise oversight over the proliferation of technologies that are primarily marketed toward law enforcement, judicial bodies, military entities, and state-level intelligence agencies. These Intrusion Software and Network Surveillance items have a more limited customer market, and are reliant on continued vendor support and opacity for continued effectiveness against security countermeasures. A review of the client lists, sales documents and statements associated with companies that are

[26] *See* Mailyn Fidler, "Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits," April 2014, http://www.lawfareblog.com/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits.
[27] WA-LIST (13) 1 04-12-2013, 3.

believed – or have themselves acknowledged – to be controlled under the proposed rules describes an industry with a limited customer base due to the high cost of such systems and added transactional discretion not characteristic of mass-market items.[28]

2. *Overlap between encryption and cybersecurity software does not negate the need to extend the TSU exception to cybersecurity software.*

It has been suggested that there is no need to apply license exception TSU to cybersecurity software because many tools used by security researchers are already controlled under the existing Category 5, Part 2 encryption controls, and as such are excluded from the General Software Note and consequently the TSU exception as well. Although we recognize that there may be some overlap between the cryptographic controls and cybersecurity software, we nevertheless believe that the TSU exception must be extended to cybersecurity software. Such an extension is necessary to address concerns that the proposed rules will adversely affect the availability of penetration testing and network security tools commonly used by security researchers.[29] Software such as CANVAS, Metasploit, and CORE Impact provide not only direct security auditing for companies, but are also used by outside contractors to test network intrusion detection systems, audit networks for vulnerabilities, and test protective measures. To the extent that these tools support cryptography, such functionality is largely ancillary to the primary purpose of the tools – they are not primarily intended for encrypted communications or cryptanalytics.

Moreover, there are identifiable cases of software and technology that appear to fall into a grey area with the proposed controls but do not include encryption. These include development suites that are used for the generation of exploits and malware.[30] As such, it is not clear that such tools would even be subject to the existing Category 5, Part 2 cryptographic controls in force today. Consequently, it does not make sense to subject all such tools to the existing restrictions on license exception TSU applied to the Category 5, Part 2 items.

[28] *See* Anderson, "Considerations on the Wassenaar Arrangement Control List Additions for Surveillance Technologies," 10-19, 23-29.

[29] *See*, e.g., Nate Cardozo and Eva Galperin, "What is the U.S. Doing About Wassenaar and Why Do We Need to Fight It?" *Electronic Frontier Foundation*, May 28, 2015, https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation; Kim Zetter, "Why An Arms Control Pact Has Security Experts Up in Arms," *WIRED*, June 24, 2015, http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/.

[30] *See*, e.g., technologies described in "Intro," https://lists.alchemistowl.org/pipermail/regs/2015-June/000173.html.

3. *The application of license exceptions should take into account the evolving role of cryptography in modern technologies.*

Although the question about whether export controls should apply to encryption technology is outside of the scope of the current request for comments, we urge the Commerce Department to recognize that such controls are also problematic for a variety of reasons, and that the new rule should not be structured in such a way that perpetuates the challenges created by these restrictions.[31] Given the issues with the existing General Software Note and related EAR carve-outs for encryption, it would be inappropriate to continue to apply these mechanisms to the newly proposed categories.

Encryption is quickly becoming a standard feature in all modern software and digital services and a norm among rights-respecting information and communications technology providers.[32] From communication systems to data storage and beyond, almost all modern software solutions recognize the importance of employing cryptographic techniques in order to protect and verify the information users generate and provide. Thus, the number of systems that risk being swept up under the controls in the existing Section 5, Part 2 restrictions is rapidly growing. Even with the myriad of reforms passed during the previous 20 years, the complexity of the rules and license exceptions surrounding cryptography in the EAR remains inaccessible to the vast majority of individuals creating software and sharing or selling it online. Much of this existing complexity and the chilling effects it promotes could be resolved by simplifying the current patchwork of license exceptions and carve-outs surrounding Category 5, Part 2.[33]

Although these challenges cannot be resolved entirely within the scope of this proceeding, BIS can at the very least ensure that the cybersecurity items are not subject to the same set of problematic restrictions. These policies should recognize

[31] This recommendation is consistent with previous recommendations that the new controls should be implemented outside of existing controls on encryption technology. *See*, e.g, Joint Civil Society Recommendations for U.S. Implementation, Part II ("Controls for Surveillance Technology Should Be Implemented Independent of Existing Encryption Controls"), 7-9.

[32] For example, the U.S. government recently mandated the use of encryption on all government websites and services (see https://https.cio.gov/). Furthermore, almost all major operating systems (e.g. Linux, Android, OSX, iOS, and Windows), storage technologies (e.g. the Ext4 filesystem (see https://lwn.net/Articles/639427/), Dropbox (see https://www.dropbox.com/en/help/27), etc), and communication systems (e.g. Google's end-to-end (see https://github.com/google/end-to-end), TextSecure (see https://whispersystems.org/), etc) now offer various forms of cryptographic capabilities.

[33] In particular, the Wassenaar Arrangement should be amended to apply mass-market and publication exceptions of the General Software Note to all encryption related controls. Similarly, the EAR should be amended to apply the 15 CFR 734.3.b and 15 CFR 740.13.d (TSU) provisions to all Category 5, Part 2 items. Such modifications would help end the current patchwork rules and requirements and remove the burdensome the registration requirements for those writing encryption-related code (which may soon include essentially all computer code).

the evolving role of encryption in modern communications tools and systems, and offer a broader range of exemptions, including those offered under license exception TSU. In doing so, BIS will also lay the groundwork for better licensing policies on software with encryption functionality in the future.

4. *Broad license exceptions will protect cybersecurity research practices and minimize concerns about scope.*

Unfettered access to mass-market and publicly available cybersecurity tools is critical to ensuring that security researchers and practitioners can adequately test systems and harden them to defend against malicious intrusion. Security researchers and professionals must be able to freely share documentation of attacks, exploit code, and exploit frameworks for purposes of penetration testing, fixing bugs, advancing protective practices, and other activities.

The free flow of this information promotes security. For example, the recent leak of the source code for Hacking Team's Intrusion Software platform has led to numerous fixes for vulnerabilities that attackers were previously able to exploit to compromise remote systems.[34] As this example demonstrates, as soon as such exploits are made publicly or widely available, they can be patched and mitigated, removing their value as effective mechanisms for exploiting remote systems. BIS should therefore aim to maximize the ability of security researchers and professionals to publicly and widely share information and software, even when it may appear to encroach on the proposed controls. Unfortunately, the proposed implementation could hinder the sharing of this crucial information, because as BIS notes in its FAQ, exploit toolkits would potentially be classified under ECCN 4D004 if they are "specially designed" or modified for the generation of "Intrusion Software."[35]

Decontrolling mass-market and publicly available tools would help alleviate some of the concerns surrounding the potential impact of the proposed implementation on security researchers and professionals, thereby forestalling the insecurity that would result from such individuals no longer having easy access to such tools.

Finally, the questions posed to BIS about the proposed rule's applicability to the exchange of exploit toolkits, amongst other challenges related to common security practices and software packages, demonstrate the ambiguity of the controls. Broadly decontrolling mass-market software and exchanges of technology will help

[34] *See* Dan Goodin, "Once again, Adobe releases emergency Flash patch for Hacking Team 0-days," *Ars Technica*, July 14, 2015, http://arstechnica.com/security/2015/07/once-again-adobe-releases-emergency-flash-patch-for-hacking-team-0-days/.

[35] BIS Intrusion and Surveillance Items FAQ #12.

BIS reduce classification requests, alleviate licensing burdens for incidentally controlled items, and allay some of the concerns of the security community.

B. Create a license exception or authorization for cybersecurity items that do not qualify for license exception TSU, but that are exported to non-government end users for defensive end uses

Certain cybersecurity items used for security research or network defense that are proprietary in nature, but do not qualify as mass-market software under license exception TSU, should merit decontrol if they are utilized for defensive purposes by non-state actors. Even with a broad license exception such as TSU in place, it is probable that some defensive security tools could be caught based on end user restrictions or restrictions imposed to limit access to only information security professionals. Nonetheless, defense-related sharing of cybersecurity items serves the public interest. We urge BIS to avoid subjecting researchers and vendors engaging in transfers for defensive purposes to an onerous licensing process in circumstances where license exception TSU does not apply. To address this, BIS should make available broad licenses to penetration testing products for extended periods of time for transfers involving non-governmental use and users where more permissive license exceptions are not available.

Examples of important defensive uses of cybersecurity items include exchanges of technology or software within corporate bug bounty programs, provision of internal access to cybersecurity items by a company or university to foreign nationals it employs or educates (which may qualify as a “deemed export”), and penetration testing services performed for non-governmental end users with the knowledge and consent of the owner or operator of that system. These uses all serve the public interest in enhancing digital security through defensive measures, and should therefore be protected.

Accordingly, a license exception or streamlined authorization process for cybersecurity items that are intended for a defensive, rather than offensive, end use should be available for exports to non-government end users. Such approach will require careful attention to end use and end user documentation requirements and evaluation processes. See section C.2 below for our recommendations on these issues.

We caution BIS against attempting to use export controls to regulate the entirety of digital threats posed by transnational criminal organizations or possible abuses of security testing or network defense systems. Such an endeavour would be inefficient and ineffective, and could come at the cost of undermining cybersecurity priorities and stifling businesses that contribute to defensive activities. While penetration testing and network security tools have the capacity to be leveraged in an offensive manner, they represent a different class of products than single-purpose surveillance technologies. The U.S. government maintains alternative mechanisms for confronting criminal and economic threats online, and should seek recourse through more clear and directly applicable legal regimes when available and appropriate.[36]

C. After adopting license exception TSU and broad license authorizations for non-governmental use and users, revise the licensing policy for remaining items to tailor it specifically to human rights concerns regarding cybersecurity items

As currently written the licensing policy of section 742.6(b)(5) is overbroad, ambiguous, difficult to properly implement, and insufficiently tailored to the specific human rights concerns that prompted the new controls. The problematic elements of the licensing policy language likely result from the breadth of items captured within the original proposed rule due to the rule's restriction on application of license exception TSU. If the TSU exception and related broad license authorizations for non-government use and users are adopted as we recommend, the licensing policy can be greatly streamlined and simplified.

While we are concerned about the implications of the proposed rules for fundamental information security practices, these concerns do not negate the history of abuse that inspired both of the proposed rules. We applaud the initiative of BIS in imposing an additional License Review Policy for Cybersecurity Items. The requirements of this policy, however, prioritize evaluative criteria that do not contribute to human rights objectives and may not be technically feasible. The Cybersecurity Items originally targeted by the Wassenaar Arrangement indeed warrant heightened scrutiny – such products are portable and once in place, they become a lasting mechanism of intrusive surveillance. There are ample cases of American-manufactured surveillance items, otherwise covered under encryption controls, being transhipped to sanctioned countries,[37] as well as examples of Intrusion Software developers claiming ignorance when their products have been used by foreign governments to spy on U.S. persons.[38] BIS should use the License Review Policy to refocus on preventing the transfer and transhipment of sensitive technologies in circumstances where they pose a risk to fundamental human rights

[36] For example, Executive Order 13694, mutual legal assistance treaty regimes, and/or domestic wiretapping statutes, as appropriate.
[37] Marquis-Boire et al., "Planet Blue Coat."
[38] "Hacking Team," *Wikileaks*, July 8, 2015, https://www.wikileaks.org/hackingteam/emails/emailid/49683.

and promoting greater accountability on the part of vendors to conduct due diligence on the end uses of the technology they are selling.

If BIS implements the license exception TSU and broad license authorizations for non-government use and users, as recommended above, decontrolling mass-market and dual-use items, it will limit the scope and types of items controlled under the rule in the first instance. In that case, we urge BIS to also adopt the following specific changes to the licensing policy.[39]

1. *The significant human rights impact of the cybersecurity items of primary concern warrants stronger review policies that apply to known repressive regimes, as well as to end users elsewhere.*

Advanced surveillance tools designed for use by law enforcement agencies and government actors require strong, across-the-board oversight to prevent use of such tools in a manner that compromises internationally recognized human rights. A presumption of favorable treatment for exports of these powerful tools to any end user, even to allied states, discredits the United States' underlying commitment to human rights. Additionally, it is not sufficient to rely strictly on Country Groups, since these classifications have not traditionally been based on human rights considerations.[40] Several countries listed under Country Group B – such as Bahrain, Ethiopia and Morocco – have been accused of using FinFisher and Hacking Team products for compromising the communications of democracy activists, including individuals based in the United States.

This approach will also have the effect of simplifying the licensing policy, obviating the need for designation of actors for special treatment and subjective interpretations that could undermine the goal of the controls. In addition to the review policies we recommend later, a presumption of denial is appropriate when the end user has a track record of violating human rights or bears a transshipment risk, wherever located.

2. *Case-by-case licensing review should require, and carefully assess, details regarding end user and end use of the cybersecurity item.*

In conducting review of license applications, BIS, the Department of State, and others involved in the review process will need to evaluate the end user and probable end use of the cybersecurity item in order to determine its potential

[39] We note that these recommendations *only* apply if BIS applies the TSU License Exception or an equivalent carveout for mass market software and similar dual-use items.
[40] "License exceptions – Supplement No. 1 to Part 740," https://www.bis.doc.gov/index.php/forms-documents/doc_download/944-740-supp-1.

human rights impact. The proposed rule should incorporate the following changes to facilitate this evaluation.

First, to the extent that BIS will rely on the term "government end-user" in the rule (or references to the inverse circumstance, e.g., non-government end-user), the definition of "government end-user" in §772.1 requires revision to account for quasi-governmental, state-captured entities that may implement state policies on surveillance and censorship. Notably, the current definition explicitly excludes "utilities (including telecommunications companies and Internet service providers)." It is well-documented that many telecommunications companies and Internet service providers are closely tied to their home governments, and may deploy surveillance tools against users on behalf of the state, either willfully or by legal compulsion.[41] To prevent artificial distinctions among end users, this exclusion within the definition should be removed, and the definition of governmental end-user broadened to include entities that are owned, operated, or otherwise subject to control by the state.

Second, the rule should reflect human rights-based due diligence requirements in §748.8(z), which lays out the unique application and submission requirements for cybersecurity items. While the EAR currently requires license applications to include identification of the actual end user and specific end use, BIS should request further details for cybersecurity items, given their demonstrated and repeated use to undermine human rights.

Previously, some of the Commenters had encouraged BIS to impose License Review Policies that:[42]

- consider consultations and post-sales support requirements and infrastructure within Intrusion Software and IP Network Surveillance license applications, such as whether the device will be located in a national backbone and questions received by the client on the usage of the system;
- maintain technical expectations about how exempted systems should operate in order to achieve legitimate and narrowly-defined objectives in order to minimize the risk of relabelling; and

[41] In both the Intrusion Software and the IP Network Surveillance cases, systems have been found embedded in the networks of telecommunications companies, compromising the traffic of Internet users; for example, the FinFisher infection proxies documented in Turkmentelecom. See "FinFisher: FinFly ISP Project, Turkmenistan," available at https://www.wikileaks.org/spyfiles/docs/GAMMA-2011-TMFinfFinF-en.pdf. In many countries of concern, legal requirements placed on telecommunications companies and ISPs to cooperate with surveillance do not adequately protect the right to privacy.

[42] Anderson, "Considerations on the Wassenaar Arrangement Control List Additions for Surveillance Technologies."

- review items not only based on their technical specification, but also their advertising material, integrations, partnerships, customers, passive operations, and end use.

Increased documentation requirements would allow for BIS to better account for differences between penetration testing tools and transfers of more sensitive technologies, while improving its overall ability to detect attempts to mischaracterize transfers. In addition to these characteristics, BIS could mandate disclosure of:

- whether the exporter maintains partnerships with Intrusion Software vendors;
- whether pertinent patents or sales material make reference to lawful interception or surveillance use cases;
- whether the system is sold as a package with Intrusion Software and whether any Intrusion Software product is reliant on the system or operation in question for operation;
- whether the product is primarily marketed to, or only sold to, law enforcement or intelligence agencies;
- whether the end recipient is a law enforcement or intelligence agency, or an entity with known relationships to such sectors;
- whether and how the vendor can account for changes in ownership or control of the item, as well as post-transfer control in the event of transhipment;
- whether the primary placement or capabilities of the device would enable its end recipient the ability to tamper with public access networks; and
- the actual network(s) on which the product is intended for deployment.

The disclosure of marketing material should be a primary component of any licensing policies for both controls. Intrusion Software and Network Surveillance systems marketed to law enforcement agencies and government actors bear striking differences from their commercial counterparts, not only in terms of support services, but also in sales material and accompanying product documentation. Moreover, these products are promoted within a broader, semi-open market for Intrusion Software systems, through tradeshows such as ISS World and Milipol.[43] The sales language and documentation offered to governmental customers will be necessarily distinct from that of defensive

[43] For more on these trade shows, see, e.g. “The Surveillance Catalog: Where governments get their tools,” The Wall Street Journal, February 7, 2012, http://graphics.wsj.com/surveillance-catalog/attendees/; Lisa Evans, “Surveillance trade shows: which government agencies attend?” The Guardian, February 7, 2012, http://www.theguardian.com/news/datablog/2012/feb/07/surveillance-shows-attendees-iss-world.

pentesting tools, based on prospective customer needs and product capabilities. Requesting such material can improve BIS's ability to incorporate human rights considerations in the course of licensing decisions, and further contribute to its ability to craft regulations that do not unnecessarily burden defensive products.

3. *Language providing for distinct treatment of "items that have or support rootkit or zero-day exploit capabilities" is unnecessary, may negatively constrain security research, and should be removed.*

The proposed rule has introduced new terminology – namely regarding rootkit or zero-day exploit capabilities – that is ambiguously understood within industry and undefined by BIS.[44] Given these ambiguities, this language should be removed. Similarly, language addressing rootkit or zero-days in "Unique application and submission requirements" and "Regional stability" licensing policies should also be removed.

As we understand, BIS's intention with these requirements is to identify the provision of high-end, pre-packaged exploits for embedding into Intrusion Software, often through subscription plans and designed for integration with a specific product. However, the publication or disclosure of security vulnerabilities frequently occurs through the release of a module for pentesting frameworks, in the same capacity that exploit brokers ship their product as modules for proprietary offensive systems.[45] As a result, it may not be possible or desirable for a product to systematically preclude support for zero-days or rootkits. Moreover, a case-by-case licensing review policy focused on end user and end use may prove more effective from a human rights standpoint than designating a subset of Intrusion Software for a presumption of denial. Instead, whether a vendor offers, or maintains partnerships with companies who do, exploit services may certainly be a characteristic germane to the license consideration process, if these terms are properly defined.

D. Provide guidance on the "generation" component of ECCN 4D004 to preclude certain classes of development tools

Common development and reverse engineering tools such as OllyDbg and Immunity Debugger present themselves as a "powerful new way to write exploits, analyze malware, and reverse engineer binary files."[46] While BIS has clarified that general purpose development tools would not be controlled as software for the

[44] Allen Householder, "Like Nailing Jelly to the Wall: Difficulties in Defining 'Zero-Day Exploit," *CERT/CC Blog*, July 7, 2015, https://www.cert.org/blogs/certcc/post.cfm?EntryID=247.
[45] "Hacking Team," *Wikileaks*, July 8, 2015, https://www.wikileaks.org/hackingteam/emails/emailid/49683.
[46] See http://www.immunityinc.com/products/debugger/.

generation of Intrusion Software, these specific tools appear “peculiarly responsible” for the generation of Intrusion Software – while otherwise not constituting the command and delivery platforms or pentesting tools noted in Cybersecurity Items FAQ #29, nor necessarily including encryption.[47] Moreover, the controlled software and technologies are not subject to the exceptions offered in the definition of Intrusion Software for hypervisors, debuggers or Software Reverse Engineering.

While these tools could be employed for the generation of malware that is used for intelligence or criminal purposes, they represent a different class of products from applications such as FinFisher’s FinSpy Agent and Hacking Team’s RCS Console. The effective difference between these two classes of products is that FinSpy Agent and RCS Console are specially designed for integration and creation of a specific Intrusion Software product.

BIS should issue guidance that differentiates and decontrols security-focused reverse engineering and exploit development platforms from those tools that are offered for the creation of the specific Intrusion Software packages, such as RCS Console.

E. Narrowly define the proposed rules on “technology” related to Intrusion Software (4E001) to control government end users and end uses, or military purposes

BIS should formally clarify the scope of the 4E001 control on “development” of Intrusion Software and establish an explicit policy that decontrols common technology transfers, narrowing the controls so that they apply *only* to end use cases and end users facilitating or conducting surveillance. This would greatly reduce controversy within the security community regarding the proposal on technology for “development” of Intrusion Software. Furthermore, decontrolling the release of technology to non-governmental uses and users would substantially reduce the immediately obvious deemed export and intercompany transfers issues.

The omission of the standard “production” or “use” from the control, in addition to outreach from BIS since the release of the proposed rule, indicates that this control was designed to be narrow. However, ongoing attempts to describe a technical line between normal research and problematic transfers may prove to be insufficient to prevent a chilling effect stemming from confusion over where that line lies. As a result, mere guidance is not enough; instead, BIS should clearly narrow application

[47] BIS, "Intrusion and Surveillance Items," http://www.bis.doc.gov/index.php/policy-guidance/faqs.

of the rule only to transfers for government end users and military or law enforcement end uses.

The Wassenaar Plenary's primary intention through 4E001.c appears to be control of commercial activities related to the preparation and integration of exploits into Intrusion Software and command and delivery platforms. In its FAQs, BIS had sought to clarify the scope of the technology for development for Intrusion Software through examples such as:

1. *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, and*
2. *Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform.*[48]

BIS further attempts to constrain the scope of the control by noting that Intrusion Software only constitutes what it perceives as a narrow subset of malware and exploits.

This technology control can be understood as attempting to control a primary component of the close and continuing relationship between Intrusion Software vendors and clients employing exploits for the compromise of remote devices. The most visible vendor of such services is the French firm VUPEN Security, whose products and research enable intermediaries to better develop and deploy Intrusion Software through providing reliable exploits. In its trade literature, VUPEN notes that:

> *Law enforcement agencies need the most advanced IT intrusion research and the most reliable attack tools to covertly and remotely gain access to computer systems. Using previously unknown software vulnerabilities and exploits which bypass Antivirus products and modern operating system protections such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) could help investigators to successfully achieve this task.*[49]

[48] BIS Intrusion and Surveillance Items FAQ #4.

[49] "Exploits for Law Enforcement Agencies," VUPEN *Security*, available at https://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf.

As we understand these services are representative of the "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices" that BIS describes in its "Scope of New Entries" and FAQ #4.[50]

There is uniform agreement between civil society and industry that export controls should incentivize responsible disclosure of vulnerabilities through primary vendors, information security firms and intermediaries conducting bug bounties. However, it remains difficult to distinguish between this "white market" and problematic, "black market" vulnerability sales based on technical data transfers alone, since the difference is primarily based on contractual arrangements and buyer.[51]

As others have noted in specific discussions about the rules:

> *When a developer sells privileged vulnerability information they typically provide compilable source code and a document describing the vulnerability in full. This is essentially the same information that someone would submit to e.g. Microsoft Security when reporting a vulnerability: a writeup, and a PoC.*[52]

The publicly released vulnerability disclosures available through platforms and organizations such as HackerOne or the Zero Day Initiative reinforce that essential security reporting does not simply entail the release of a binary exploit, and requires complementary documentation and discussion.[53] Even further, the process of determining whether an exploit can be developed to "reliably and predictably defeat protective countermeasures and extract information" is frequently a pressing security question.[54]

[50] According to the "Scope of New Entries" section of the rule proposed by BIS on May 20, 2015, "Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, Intrusion Software include network penetration testing products that use Intrusion Software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of Intrusion Software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices. The new entry on the CCL that would control Internet Protocol (IP) network communications surveillance systems or equipment is restricted to products that perform all of the functions listed; however, the Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry;" BIS Intrusion and Surveillance Items FAQ #4.

[51] Mailyn Fidler, "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis," April 2014, http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-Review-Changes-Made.pdf.

[52] "On Definitions and Limits," https://lists.alchemistowl.org/pipermail/regs/2015-June/000249.html.

[53] "XXS in Dropbox main domain," https://hackerone.com/reports/59356.

[54] The Heartbleed vulnerability provides an illustrative example. Upon release of the vulnerability, there were open questions about whether the issue could be reliably employed to extract private keys from a remote system (qualifying under the Intrusion Software criteria). After an open challenge by Cloudflare and others, cooperation between private companies and researchers lead to the development of more reliable exploitation of the Heartbleed vulnerability. While this example would have been decontrolled by the General Technology

The challenges of establishing a strictly technical definition of problematic transfers were made more clear by the product information and communications between Hacking Team and exploit brokers, such as VUPEN and Netragard. These emails clearly demonstrate a private market for the sale of exploits to the highest bidder; however, the information shared with Hacking Team for marketing and sales of vulnerabilities by these vendors are not substantially different from the information disclosed in a critical vulnerability (CVE) report.[55]

Beyond the inherent risks of overbreadth, the pursuit of a strictly technical line of difference between security research and exports of concern will limit the ultimate effectiveness of such control. The primary value provided by exploit brokers is information on the nature of a vulnerability – the proof of concept that BIS has repeatedly asserted is not controlled. In very few circumstances is more required to understand and replicate an attack than access to a proof of concept or working exploit. A proof of concept "shellcode" can be replaced by functional "shellcode" for the compromise of the device.[56] Permitting release of proof of concepts while controlling technical data on exploit techniques becomes a futile endeavour, as it will be easy to discern mechanisms from source code or decompiled binaries. In fact, much of the learning process occurs from reverse engineering of exploits found in the wild, even in the case of sophisticated Intrusion Software built by state actors.

Some elements of the security industry appear to be open to regulations that create clear and consistent expectations about responsible behavior. For example, Netragard has acknowledged that it was unaware of the end use and end users of its Exploit Acquisition Program, and publicly stated that the "zero-day exploit market needs to be thoughtfully regulated," adding that:

> *[R]egulations should provide a framework for the legitimate sale of 0-day exploits. They should establish a set of guidelines to help control who can responsibly purchase 0-day exploits. Such regulations would make our jobs as ethical 0-day exploit brokers much easier and far less risky.*[57]

As with licensing policy, in considering end use and end users, strictly controlling against "military end use" or governmental users may not be sufficient. This

Note, this is representative of common practice that often is not public and may not be covered as fundamental research.

[55] "Hacking Team," *Wikileaks*, July 8, 2015, https://www.wikileaks.org/hackingteam/emails/emailid/49683.

[56] Ivan Arce, "On the Quality of Exploit Code," RSA *Conference* 2005, http://www.coresecurity.com/system/files/HT2-301-IvanArce-v1.1.pdf.

[57] Adriel Desautels, "The HackingTeam Breach & EAP," *Netragard*, July 2015, https://www.netragard.com/the-hackingteam-breach-eap.

approach will pose a few challenges; namely in protecting disclosure to CERTs, other entities responsible for formal disclosure processes, or for government-provided services. This requires nuance, however, since such entities may also be compelled to disclose vulnerability information to intelligence agencies. This necessitates end use controls, in addition to end user limitations, due to the diverse ways that "government end user" might be too narrow.

F. Narrowly defined rules for technology necessitate clear "Know Your Customer" guidance

As with other industries, "Know Your Customer" policies are processes built around detecting and responding to a series of criteria (or "red flags") that could indicate potentially suspicious transactions. The Department of Commerce is aware that sensitive technologies are often at risk for transhipment or illicit trade, and has a history of providing industry-specific guidance to exporters to address these types of concerns.[58] In the absence of clear guidance regarding the export surveillance technology – and as an attempt to promote industry self-regulation – civil society organizations and multi-stakeholder initiatives have offered their own recommendations, based on experiences and best practices, as well as international norms such as the UN Guiding Principles on Business & Human Rights.[59] Examples of detailed suggestions on developing a "Know Your Customer" regime appropriate for censorship and surveillance technologies have been documented by the Electronic Frontier Foundation and the Global Network Initiative, including recommendations on the scope and structure of the process and key definitions.[60]

Given the narrow scope of the proposed Intrusion Software control, "Know Your Customer" guidelines and related due diligence are critical to ensure that the rule still has the intended effect of preventing the transfer of technology that can be used to facilitate human rights abuses. At a minimum, in evaluating whether a technology may be used for repressive purposes, companies, organizations or individuals should assess the likely end use and end user of a product with reasonable certainty. These processes should include providing documentation

[58] *See* "Know Your Customer Guidance," *U.S. Department of Commerce's Bureau of Industry and Security*, https://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/freight-forwarder-guidance/23-compliance-a-training/47-know-your-customer-guidance.

[59] UN, "Guiding Principles on Business and Human Rights," 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[60] Cindy Cohn and Jillian C. York, "'Know Your Customer' Standards for Sales of Surveillance Equipment," *The Electronic Frontier Foundation*, October 24, 2011, https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment; Cindy Cohn, Trevor Timm, and Jillian C. York, "Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes," *Electronic Frontier Foundation*, April 2012, https://www.eff.org/document/human-rights-and-technology-sales.

describing the nature of the due diligence conducted and responses from the end recipient.

Such documentation may include, but is not limited to:

- Relationship with the contracting entity, including length of relationship, contractual mechanisms for compliance, and demonstrated history of compliance with contractual and legal obligations;
- Final country destination, recipient, and end use of the technology, such as location in a network or nature of the buyer, supported by clear and detailed documentation;
- Extent of ongoing servicing of the technology, including potential for post-export checks on compliance; and
- Design of the technology and customizations.

To aid in compliance with these requirements, the Department of Commerce should provide specific lists of possible red flags that illustrate the type of circumstances that should cause reasonable suspicion that a transaction will violate the new controls for cybersecurity items.

Relevant red flags may include:

- Originating IP addresses for software updates or other forms of communications, which may indicate that a product has been transferred or resold to another entity;
- Language requirements and device support requests;
- Provision of equipment that vastly exceed the traffic requirements for the stated installation location; and
- Qualifications and background of participants present at training sessions.

The Commerce Department should emphasize that “Know your Customer” encompasses “know your reseller” and “know your regional partners,” which will help mitigate the risk that companies attempt to “self-blind” by ignoring public research, records on the location of service and update requests, and indications of the actual end uses reflected by customers’ requests. The activities of FinFisher and Hacking Team demonstrate that companies have had little incentive in the past to perform due diligence or respond to reports of abuse, creating a “race to the bottom” that disincentivizes better behavior in the broader industry. It is not sufficient for a company to perform “Know Your Customer” checks without taking reasonable steps to determine whether the technology in question is likely to be transferred from the original customer to end users in repressive countries who may use it for nefarious purposes.

The Commerce Department should also consult with industry and civil society to promote implementation of "Know Your Customer" policies that will reduce the potential for approved exports to be misappropriated for the abuse of human rights. Recurring outreach will also help ensure that the Commerce Department's efforts match the fast pace of technological development and also address evolving ways in which infringing parties may attempt to bypass the controls.

G. Issue clear guidance on key terminology introduced into the text of the rule

In order to minimize ambiguity and clarify enforcement objectives, BIS should issue clear definitions regarding the terminology used in future proposed and final rules. Currently, the proposed rule uses a number of terms of art that are either poorly defined or not defined at all. Adding to the confusion, many of these terms lack widely-agreed upon definitions in the technical community. Such terms must either be clearly defined, or removed from the text of the proposed rule.

As noted previously, our concerns include the use of the terms "rootkit" and "zero-day exploit capabilities" found in the License Review Policy for Cybersecurity Items section of the draft rule and the proposed additions to 15 CFR 742.6.[61] Both of these terms are undefined by BIS and have no agreed-upon definition in the technical community.[62] Furthermore, as BIS has acknowledged, some of the terms or functions included in ECCN's 5A001.j definition are not defined, including "carrier class IP network," "indexing of extracted data," and the basis of the "relational network" mapping within the control. BIS should explicitly define these terms – and where appropriate provide examples of their meaning – in any final rule that it issues.

Failing to define such terms will result in a rule that has an unnecessary chilling effect on good faith security research because of ambiguity about what can and what cannot be legally exported. We have already seen the detrimental result of poorly-defined terminology on the security research community in other areas of U.S. law, and urge BIS to avoid making the same mistakes in this proposed rule.[63]

[61] 80 FR 28853. "License Review Policy for Cybersecurity Items"; 80 FR 28853. "§ 742.6 Regional stability."

[62] For example, some in the community define the term "zero-day" to refer to any vulnerability that has not been publicly released. Other use the term to refer to any unpatched vulnerability. Likewise, the term "rootkit" has a range of meanings, from special software installed at the firmware level to manipulate a normally installed operating system. Other use the term to refer to any software that tries to mask its existence from the user.

[63] For example, the ambiguities surrounding the rights of security researchers under Section 1201 of the Digital Millennium Copyright Act (17 USC 1201) continue to stymie good faith research and force researchers to seek

Clear definitions of key terms would also provide for the basis of a better understanding and more efficient uses of the license exceptions proposed previously.

Given the complexity of the rule, we similarly urge BIS to include language in its "Scope of the New Entries" section explicitly noting the forms of security research (both public and proprietary) that are outside the scope of the controls. Specific examples of controlled or decontrolled products or software would be welcome and would assist the software development and security communities – whose members are generally unfamiliar with the nuances of export controls – in properly interpreting the proposed rule.

H. Issue an amended version of the proposed rule on Intrusion Software prior to publication of the final rule

We appreciate BIS's initiative in publishing the proposed rule and requesting comments, and its willingness to provide opportunities for clarifications on the language. The open and iterative process that public comments enable lead to better rules, and have already had a demonstrable impact by avoiding the numerous issues that would have arisen had BIS simply published a final rule without first seeking input from the public. In light of the numerous concerns outlined in these comments, and the significant revisions that addressing them will likely entail, we request that BIS amend the proposed rules and issue a second request for comments prior to publishing a final rule. We note that this is not a request to extend the current comment period, nor do we believe that BIS will be unable to resolve the issues that we have noted within the constraints of the language that the United States has committed to implement as a Wassenaar member. Instead, issuing a revised draft rule and seeking additional comments will simply ensure that the concerns that commenters have outlined have been adequately and appropriately addressed prior to publication of a final rule. This second proposed rule should include specific information on license exceptions and definitions of key terms, which were omitted from the first proposed rule, in order to allow affected communities and industries to fully assess the impact of the rules on their commercial operations and articulate their concerns through public comment.

changes to the law; *see* Copyright Office Hearing on "Library of Congress Sixth Triennial Rulemaking: Class 25," May 26, 2015.

I. Establish an iterative process to see how the rule evolves in implementation

Public debates about the role of regulation in impeding the proliferation of surveillance and censorship equipment have often hinged on whether export control agencies are responsive enough to adapt to changes in technology and industry norms. While these controls are intended to define single-purpose surveillance products, rather than dual-use technologies such as deep packet inspection equipment, the subsequent reaction to BIS's proposed rules demonstrates an increased need for continued consultations between government agencies and representatives from industry, technical communities, academia and civil society. Over time, changes in cybersecurity technology may warrant additional license exceptions – or even narrowing of licenses – for these rules, as well as for encryption and communication intercepting devices controls.

As an example, it may be necessary in the future to add Network Intrusion Detection to the excluded design purposes under the IP Network Surveillance systems control. Network intrusion detection systems, such as Bro, Snort, and other commercial products, are becoming increasingly critical for maintaining the security of modern networks. While we do not feel that such tools as currently crafted will be subject to the proposed 5A001.j rules, it is possible that future advances in technology might create ambiguities about whether or not they are controlled. For the purpose of this comment period, ensuring that the new categories are subject to the TSU and clarifying the definition of some of the terms of art discussed previously will help alleviate these concerns, but in the long-term ongoing consultations to ensure that the controls continue to be appropriately tailored as the technology evolves will likely be necessary.

V. Conclusion

We would like to reiterate our gratitude to the Bureau of Industry and Security for publishing the proposed rule for comment and for considering the recommendations submitted here. We hope that we have offered insight that will lead to a final rule that addresses the human rights concerns posed by the spread of the single-use surveillance technologies without adversely affecting a variety of additional technologies, including important security research tools.

We continue to believe that it is possible to implement the 2013 Wassenaar controls related to surveillance technology in a timely manner that balances both the human rights concerns that prompted these controls and the important goal of preventing security researchers and professionals from being subject to overbroad restrictions that could have a chilling effect on their activities. In order to achieve that balance, we urge the Commerce Department to carefully consider draft language and continue to consult with a broad range of civil society, academic experts, and security professionals to ensure that unintended consequences are mitigated to the greatest extent possible without sacrificing the important policy goals advanced by the original rules.

In the event that a final rule threatens to be either overinclusive or underinclusive in the technologies that it controls, we believe that it is better to err on the side of underinclusion, potentially excluding some surveillance technologies that might warrant control but can be addressed using other policy options besides export controls. BIS can revisit the controls in the future if they need to be amended. However, we are optimistic that it is possible to strike the right balance and look forward to working with the Commerce Department to achieve that goal.

Thank you for your consideration.

Respectfully submitted,

Access
Center for Democracy & Technology
Collin Anderson
Electronic Frontier Foundation
Human Rights Watch
New America's Open Technology Institute