Cyber-surveillance export control reform in the United States



Various factors suggest the US government may soon update US export controls on intrusion software, network surveillance systems, and intelligence-collection tools. Peter Lichtenbaum, David W. Addis and Doron O. Hindin consider what may be forthcoming.

Based on recent US agency actions and statements, the US government is likely to update soon its export controls on intrusion software (including exploit research), network surveillance systems, and intelligence collection tools.

Collectively, these items consist of equipment, software, and technologies designed to gain access to, surveil, and control third-party electronic devices. These highly effective tools are increasingly being used for nefarious purposes, such as by 'black hat' hackers to steal sensitive information and extort corporations and private individuals, and by authoritarian government regimes to repress dissidents. However, such products are also routinely used by 'white hat' cybersecurity specialists to protect systems and data as well as by legitimate government intelligence and law enforcement agencies to achieve critical national security objectives.

As background, and as discussed further below, the US Commerce Department sought in 2014-15 to limit the proliferation of these items through proposed export control regulations on 'intrusion software' and 'IP network communications surveillance systems,' but that regulatory endeavour lapsed in 2016 in the face of resolute opposition by industry and civil society.

However, the US government has maintained its overall objective of regulating cyber-surveillance and intelligence-gathering tools through export controls. To that end, the Commerce Department and State Department are working toward a series of regulatory changes that, in the aggregate, would significantly change export controls over cyber and intelligence products.

This article surveys these regulatory developments and evaluates what to expect from the US government in the months ahead.

Wassenaar cyber-surveillance controls and US exceptionalism

In December 2013, the cyber industry was caught by surprise when, as a result of proposals by France and the United Kingdom, the Wassenaar Arrangement's List of Dual-Use Goods and Technologies and the Munitions List (collectively, the 'Wassenaar List') was amended to cover, for the first time, 'intrusion software' and 'IP network communications surveillance' systems.[1] This proposal was made as a result of concerns from non-government organisations that certain repressive governments were able to use such software and systems to eavesdrop on dissidents and reporters within their societies.

The US government has maintained its overall objective of regulating cyber-surveillance and intelligence-gathering tools through export controls.

The new 2013 language covered commodities, software, and technology for the generation, operation, or delivery of, or communication with, 'intrusion software,' defined as:

> Software specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures, of a computer or network-capable device, and performing any of the following:
>
> (a) The extraction of data or

information, from a computer or network-capable device, or the modification of system or user data; or

(b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

(Notes and quotation marks omitted)[2]

In addition, the updated 2013 Wassenaar List covered communications surveillance systems, and related commodities, software, and technologies, specially designed to extract, index, search, and map metadata from carrier class IP networks, such as national grade IP backbones.[3]

The controls over intrusion software and IP network communications surveillance systems were immediately implemented by the export control authorities of a number of countries for which the Wassenaar List is self-executing. In other countries, the Wassenaar List requires subsequent implementing legislation, but is then generally adopted verbatim, such as in the European Union.[4]

By contrast, the United States does not automatically adopt Wassenaar List amendments. Rather, after amendments are adopted at annual Wassenaar plenary meetings, the US government launches an interagency review process, which routinely involves seeking industry comments, to determine national security, foreign policy, and economic impacts of the Wassenaar amendments. Following that process, the US government typically adopts the amendments, but frequently modifies the language to reflect US-specific interests and so that it fits neatly within either the Commerce Control List ('CCL') – administered by the US Department of Commerce, Bureau of Industry and Security ('BIS') pursuant to the Export Administration Regulations ('EAR') – or the US Munitions List ('USML') – administered by the Department of State, Directorate of Defense Trade Controls ('DDTC') pursuant to the International Traffic in Arms Regulations ('ITAR').

The US government took this approach with respect to Wassenaar's 2013 cyber-surveillance amendments. Ultimately, in May 2015, BIS published a proposed rule to incorporate the 2013 Wassenaar intrusion software controls into CCL category 4 and the controls over IP network communications surveillance systems into CCL category 5 part 1.[5]

BIS's proposed rule elicited a deluge of public comments from industry and civil society. Many of the commenters expressed serious concern that because the Wassenaar language was, in their view, overly broad, its incorporation into the CCL would chill global 'white hat' exploit and vulnerability research and would otherwise undermine US national security and economic interests.[6] For example, commenters presented BIS with hypothetical scenarios in which exploit researchers uncover vulnerabilities in software platforms of foreign vendors but are then prevented from immediately notifying those vendors of the risks, due to a requirement to first obtain export controls licensing from BIS. Similarly, commenters argued that the proposed rule could unjustifiably require victims of rootkit or other malicious software attacks to obtain licensing prior to sharing their infected device with non-US forensic specialists.[7] Others explained that adopting the Wassenaar language would be counterproductive to US national security and economic interests by imprudently controlling general purpose programming environments, such as integrated design environments, and commonly used defensive cyber tools, such as penetration testing products, adaptable end point detection and response tools, auto-updating antivirus and antimalware programs, and forensic exploit toolkits.[8]

As explained by BIS in a recent FAQ, US government efforts have been successful in negotiating limited changes to the Wassenaar List.

The industry concerns prompted BIS to publish 32 clarifying frequently asked questions ('FAQs'), which in turn prompted yet further industry pushback.[9] Ultimately, the force of the industry concern resulted in a 2016 letter by then-Secretary of Commerce Penny Pritzker to cyber industry representatives notifying them that in light of industry feedback and input from Congress, academia, and civil society, the United States would not implement the Wassenaar 2013 intrusion software controls.[10] The letter further committed that the US government would advocate at upcoming Wassenaar plenary meetings for the Wassenaar List to be amended by deleting the intrusion software controls in their entirety.

To date, the intrusion software controls in the Wassenaar List have not been eliminated.[11] However, as explained by BIS in a recent FAQ, US government efforts have been successful in negotiating limited changes to the Wassenaar List, 'in order to minimize the negative impact the [intrusion software] entries would have.'[12]

A particularly significant development that the FAQ attributes to US negotiation efforts is that as of 7 December 2017, the Wassenaar List now clarifies that the technology controls on intrusion software 'do not apply to "vulnerability disclosure" or "cyber incident response", new terms of art in the Wassenaar List with corresponding definitions.[13] This important clarification provides welcome relief to vendors worldwide, who are often mandated by contract or by prevailing regulation to respond without delay to data breaches. The change also offers a needed safe-harbour for exploit researchers and cybersecurity specialists worldwide who can now receive, analyse, and remediate vulnerabilities without delay.

A second change to the Wassenaar List discussed in the BIS FAQ is that the list now clarifies that software that provides updates or upgrades that are authorised by the owner or operator of the target system would not be controlled as intrusion software, as long as the software itself was not specially designed to update intrusion software or command and delivery

platforms for intrusion software.[14] That clarification was necessary to avoid unnecessarily controlling general purpose design environments, auto-updating anti-virus tools, and other pervasive and commercially available software tools, while focusing controls only on more aggressive command and delivery platforms for intrusion software, such as exploit toolkits and penetration testing tools.[15]

Shortly after these Wassenaar changes were agreed to, Rob Joyce, the White House cybersecurity coordinator at the time, praised the US negotiating achievements: 'We applaud the hard work of the US interagency and our partners in industry, the research community, and foreign governments to clarify software and technology controls that could have had a negative impact on legitimate cybersecurity.'[16]

However, notwithstanding these negotiation successes, BIS has acknowledged that they are only an initial step towards addressing the concerns raised in response to its 2015 rulemaking proposal, and that a number of alternative next steps remain possible:

'We have not decided on a next step yet [concerning intrusion software]. There are a range of possible actions we could take, including returning to Wassenaar in 2018 to negotiate further changes to the text, publishing a rule to implement the text, or publishing a notice of inquiry or proposed rule for further comment.'[17]

Subsequently, on 24 October 2018, BIS finalised implementation of the 2017 Wassenaar List. To the continued relief of the cybersecurity industry, neither Wassenaar's category 4 intrusion software nor its category 5 part 1 IP network communications surveillance entries were incorporated in the CCL.

However, BIS's recent CCL update, which implements the most current Wassenaar List but continues to exclude that list's controls over cyber-surveillance tools, by no means signals a retreat by the US government from asserting control over those tools. In fact, other regulatory developments, surveyed below, signal the opposite: cyber-surveillance applications, including exploit research, may be the subject of a broad regulatory reform.

ECRA foundational technologies – comment period

On 13 August 2018, Congress enacted the Export Control Reform Act of 2018 ('ECRA'), which established a formal interagency process to identify and regulate emerging and foundational technologies that are deemed 'essential to the US national security' and are not otherwise controlled for export purposes.

The Secretary of Commerce reportedly informed the Congressional-Executive Commission on China by letter that by the autumn of 2018, the Department of Commerce would propose new 'human rights controls for the 21st century'.

The interagency process established under ECRA has already led to a 19 November 2018 publication in the Federal Register of an advance notice of proposed rulemaking for the 'Review of Controls for Emerging Technologies.'[18] As described in the notice's preamble, BIS

'seeks public comment [by 10 January 2019[19]] on criteria for identifying emerging technologies that are essential to US national security, for example because they have potential conventional weapons, *intelligence collection*, weapons of mass destruction, or terrorist applications or could provide the United States with a qualitative military or *intelligence advantage*.' (Emphases added)

In addition, a specific category of representative emerging technologies proposed in the notice is: 'Advanced surveillance technologies, such as: Faceprint and voiceprint technologies.'

Commerce will publish a separate notice of proposed rulemaking related to 'foundational' technologies, which could also potentially encompass cyber-surveillance tools and technologies.

The emphasis in the November notice's preamble on intelligence collection and the US intelligence advantage, and the inclusion of a dedicated emerging technology category of '[a]dvanced surveillance technologies,' relates directly to the government's ongoing efforts at leveraging export controls to curtail the proliferation of intrusion software and surveillance technologies.

As discussed above, the 2013 Wassenaar cyber-surveillance amendments originated from proposals by European governments and the US government yielded to the barrage of public disapproval that they generated. By contrast, under ECRA, the US Congress has explicitly directed the US administration to identify, and impose export controls on, emerging and foundational technologies, which the government has in turn interpreted to include advanced surveillance technologies, including for intelligence collection purposes. With ECRA as its tailwind, the US government might be more determined to impose controls on cyber-surveillance items, particularly if these controls are limited based on the Wassenaar amendments discussed above.

Human rights export controls for the 21st Century

On 9 May 2018, and in parallel to ECRA developments, Senator Marco Rubio and Representative Chris Smith, on behalf of the Congressional-Executive Commission on China ('CECC'), transmitted a letter to Secretary of Commerce Wilbur Ross identifying that compelling evidence indicates that, notwithstanding current US export controls, US companies are selling Chinese authorities advanced products used for 'surveillance, detection, and censorship'.[20] The congressmen in the letter explicitly asked the Secretary to explain what 'new legislation or new authorities [are] needed to revisit/revise export control regulations so they are

Cyber surveillance

consistent with the rapid evolution of technology,' and whether any 'software or technology which could be used for the purpose of domestic repression, [is] subject to export controls with respect to Chinese end-users of concern?'

These concerns and the need to 'revisit/reform export control regulations' were echoed in CECC's 2018 annual report, published on 10 October 2018, which recommends that the US administration 'Revamp Export Controls,' including by amending the USML to include 'new technologies… [that] enhance surveillance and the ability of security forces to repress universally recognized human rights.'[21]

In response, the Secretary of Commerce reportedly informed CECC by letter that by the autumn of 2018, the Department of Commerce would propose new 'human rights controls for the 21st century'. The concept would be to update the Commerce Department's so-called 'Crime Controls', under which the department regulates items of traditional human rights concerns such as leg shackles, thumbscrews and police batons. The new proposal would focus on high-technology items that can facilitate human rights abuses. It is unclear how this development would relate to the ECRA rulemaking discussed above, but it may provide a more expedited vehicle for Commerce to control intrusion software platforms or surveillance tools, compared with the ECRA process. In particular, this could be the case with respect to software items that are long-established technologies, since the ECRA process for identifying 'foundational' technologies has not yet even started. Even the ECRA 'emerging' technologies process will probably not result in an actual proposed rule until sometime in 2019. By contrast, the 'human rights' rulemaking is expected to involve publication of a proposed rule in December 2018.

USML category XI(b)

A further indication of forthcoming controls on intrusion software and surveillance technologies was DDTC's announcement on 30 August 2018, of a 12-month extension of the application of USML category XI(b), in order to provide DDTC with the opportunity to complete a 'wholesale revision of USML category XI.'[22] Category XI(b) – the scope of which has been the subject of ongoing interagency debate and numerous rulemaking processes[23] – is the principal USML entry intended to capture national-level intelligence collection tools:

> * [XI](b) Electronic systems, equipment or software, not elsewhere enumerated in this subchapter, specially designed for intelligence purposes that collect, survey, monitor, or exploit, or analyze and produce

Links and notes

1 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies is a multilateral organisation with 42 member states, and several other non-member observers, that collaborate on export controls.

2 Wassenaar List (2013), Category 4.A.5.

3 Wassenaar Category 5.A.1.j.

4 The European Union, for example, adopted the 2013 Wassenaar List controls on 22 October 2014. See: Commission delegated regulation, (EU) No. 7567/2014 (Oct. 22, 2014), at http://ec.europa.eu/transparency/regdoc/rep/3/2014/EN/3-2014-7567-EN-F1-1.PDF, entering into force on December 31, 2014, pursuant to Commission delegated regulation (EU) No. 1382/2014, OJ L 371/1, (30 December 2014).

5 Department of Commerce, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, Proposed Rule with Request for Comments, 80 Fed. Reg. 28553 (20 May 2015).

6 See e.g., Comments to the US Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements (RIN 0694-AG49) On Behalf Of Access, Center for Democracy & Technology, Collin Anderson, Electronic Frontier Foundation, Human Rights Watch, and New America's Open Technology Institute (20 July 2015), available at https://www.eff.org/files/2015/07/21/jointwassenaarcomments-final-1.pdf.

7 See https://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf http://trade.ec.europa.eu/doclib/docs/2017/december/tradoc_156502.pdf

8 See e.g., BIS 2015 'Intrusion and Surveillance Items Frequently Asked Questions ('FAQ'),' at FAQs 8, 12, 16, and 29, available as an archived webpage at: https://web.archive.org/web/20150908025350/https://www.bis.doc.gov/index.php/policy-guidance/faqs?view=category&id=114#subcat200.

9 Id; See Mailyn Fidler, Proposed US Export Controls: Implications for Zero-Day Vulnerabilities and Exploits at Lawfareblog.com (10 June 2015), available at, *https://www.lawfareblog.com/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits*

10 Letter From The Honorable Secretary of Commerce, Ms. Penny Pritzker, To American Petroleum Alliance (API), et. al. (1 March 2016), available at https://www.bis.doc.gov/index.php/forms-documents/about-bis/newsroom/1434-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrang/file.

11 Tami Abdollah, *US fails to renegotiate arms control rule for hacking tools,* Associated Press (19 December 2016), available at https://apnews.com/c0e437b2e24c4b68bb7063f03ce892b5 (noting that initial attempts in 2016 at renegotiating the controls were unsuccessful); Garett Hinck, *Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research* (5 January 2018), available at https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-resear (surveying the US negotiating efforts to date and resultant changes in December 2017 to the Wassenaar List).

12 BIS, 'Intrusion and Surveillance Items,' FAQ No. 1, at, https://www.bis.doc.gov/index.php/policy-guidance/faqs#faq_62 (visited 20 November 2018).

13 Wassenaar List Category 4.E.1. (defining a 'vulnerability disclosure' as 'the process of identifying, reporting, or communicating a vulnerability to, or analysing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability' and defining a 'cyber incident response' as 'the process of exchanging necessary information on a cybersecurity incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident').

14 BIS, 'Intrusion and Surveillance Items,' FAQ No. 1, at, https://www.bis.doc.gov/index.php/policy-guidance/faqs#faq_62 (visited 20 November 2018).

15 See e.g., BIS 2015 'Intrusion and Surveillance Items Frequently Asked Questions ('FAQ'),' at FAQs 8, 12, 16, and 29, available as an archived webpage at: https://web.archive.org/web/20150908025350/https://www.bis.doc.gov/index.php/policy-guidance/faqs?view=category&id=114#subcat200.

16 Shaun Waterman, The Wassenaar Arrangement's latest language is making security researchers very happy *in* cyberscoop.com (20 December 2017), available at, https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

17 BIS, 'Intrusion and Surveillance Items,' FAQ No. 1, at, https://www.bis.doc.gov/index.php/policy-guidance/faqs#faq_62 (visited 20 November 2018).

18 Department of Commerce, *Review of Controls for Certain Emerging Technologies; Advance notice of proposed rulemaking (ANPRM)*, 83 Fed. Reg. 58201 (19 November, 2018).

19 The comment period was initially scheduled to close on December 19, 2018, but was extended by three weeks in response to requests by leading technology companies that they be allotted additional time for drafting comments

20 See Letter From Senator Marco Rubio and Representative Chris Smith, Co-Chairs of the Congressional-Executive Commission on China, To The Honorable Wilbur Ross, Secretary of Commerce (9 May 2018), available at https://www.cecc.gov/media-center/press-releases/chairs-ask-commerce-secretary-ross-about-sale-of-surveillance-technology.

21 CECC, Annual Report, 2018, p. 16, available at https://www.cecc.gov/sites/chinacommission.house.gov/files/Annual%20Report%202018.pdf.

22 Department of State, *Continued Temporary Modification of Category XI of the United States Munitions List; Final rule; notice of temporary modification*, 83 Fed. Reg. 44224 (30 August 2018).

23 Department of State, *Amendment to the ITAR: USML Category XI (Military Electronics), and Other Changes; Final Rule*, 79 Fed. Reg. 37536, 37544 (1 July 2014) (proposing XI(b) controls that excluded the phrase 'analyze and produce information from' and that controlled only 'systems or equipment,' but not software); Department of State, *Temporary Modification of Category XI of the USML; Final rule; notice of temporary modification*, 80 Fed. Reg. 37974, 37975 (2 July 2015) (explaining that as a result of the 2014 version of XI(b), DDTC grew concerned 'that exporters may read the revised control language [in Category XI(b)] to exclude certain intelligence analytics software that has been and remains controlled on the USML.').

24 Department of State, *Continued Temporary Modification of Category XI of the United States Munitions List; Final rule; notice of temporary modification*, 83 Fed. Reg. 44224 (30 August 2018).

information from, the electromagnetic spectrum (regardless of transmission medium), or for counteracting such activities.[24]

Currently, the broad formulation of category XI(b) serves as a strong hook for the US government to control sensitive intrusion software platforms or IP network surveillance technologies. At the same time, category XI(b)'s fairly abstract language has also historically provided exporters with tenable arguments to justify self-classifications of intelligence collection items under BIS jurisdiction, to the extent those items are more accurately described in the CCL. A discussion of the numerous surveillance- and intelligence-related export control classification numbers on the CCL, as well as BIS's policies governing surreptitious listening and cryptographic or cryptanalytic items, is beyond the scope of this article. Nonetheless, it is worth noting that these Commerce Department controls and policies, and attendant licence exceptions, have proven relevant for various vulnerability software and surveillance tools that may routinely be sold to local law enforcement or private security firms and that are more precisely captured under the EAR, and not under the ITAR's USML category XI(b) controls.

However, that all may change with the as-yet-unknown ramifications of DDTC's 'wholesale revision of USML Category XI'. The DDTC's undertaking with respect to category XI should be viewed in conjunction with the Wassenaar, ECRA, and China Commission developments discussed above, which collectively signal forthcoming export controls over intrusion software and surveillance technologies.

Conclusion

The confluence of efforts by the US delegation at Wassenaar; pending ECRA rulemaking on emerging technologies, and the expected similar ECRA rulemaking on foundational technologies; encouragement by Congress for revised Commerce Department 'human rights controls for the 21st century'; and impending revisions of USML category XI(b) by the State Department, collectively signal a forthcoming reform in US export controls over intrusion software (including potentially exploit research), network communications surveillance systems, and intelligence-collection tools.

Those likely to be most affected by such reforms should closely monitor the concurrent agency processes discussed above. Stakeholders should also consider proffering feedback and insights to government, so that the emerging rules appropriately reflect values of human rights, national security, foreign policy and economic interests.

Peter Lichtenbaum, David W. Addis, and Doron O. Hindin are attorneys in the International Trade practice at Covington & Burling LLP. Mr. Lichtenbaum previously served as Assistant Secretary of Commerce for Export Administration.

plichtenbaum@cov.com

daddis@cov.com

hindind@cov.com

This article first appeared in the December 2018 issue of WorldECR, the journal of export controls and sanctions.

www.worldecr.com