Background

This comment is submitted by Privacy International in response to the proposed rule (RIN 0694-AG49) implementing controls on intrusion and surveillance items agreed within the Wassenaar Arrangement in 2013.

Privacy International, a registered UK charity (No. 1147471), was founded in 1990 and was the first organisation to campaign at an international level on privacy issues. Privacy International ("PI") envisions a world in which the right to privacy is protected, respected, and fulfilled. Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.

Part of the work that Privacy International does is to investigate the secret world of government surveillance and expose the companies enabling it. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

Throughout our history we have proactively engaged with and rigorously campaigned on issues relating to export restrictions. Throughout the 1990s, when governments were trying to restrict individuals' access to encryption, together with the wider privacy community, we fought against such restrictions, highlighting the threat that such measures pose to individual privacy and the security of our modern technological infrastructure.

More recently, we have campaigned for export restrictions to apply to surveillance technologies which represent a fundamental risk to privacy and a range of other human rights. PI coordinates a global coalition aimed at ensuring surveillance technologies are not used to facilitate human rights abuses or internal repression. The Campaign Against Unlawful Surveillance Exports brings together human rights, arms control, tech policy, and media freedom civil society groups to campaign for stronger safeguards to prevent the use of surveillance technologies in ways that undermine fundamental human rights.

We therefore welcome initiatives aimed at achieving greater oversight of the trade in surveillance technologies, including the 2013 agreement at the plenary of the Wassenaar Arrangement (WA) to include IP Network Surveillance Systems and items related to intrusion software on the dual use control list. Since then, we have been closely monitoring the implementation of the controls by participating states.

It is evident that export control policy and international cooperation on export controls stems historically from strategic state decision-making related to national security and foreign policy interests. The core criteria for including an item within control lists include the ability to make a clear and objective specification of the item. This objective specification becomes increasingly difficult where technology underpinning surveillance equipment is similar, and in some cases the same, as that used within commercial and civilian applications and techniques. While this is a common issue within dual use export regulation, the potential for regulations within the computer and telecommunications network security context to have negative consequences upon individuals and IT security research makes regulatory measures within this field particularly challenging and vitally important to get right in a clear and concise manner.

Nevertheless, if export regulations and international cooperation in export policy are to remain a relevant mechanism for fostering human rights and international security, it is essential that they are updated to take into account new technologies while protecting security research and the free flow of information. We believe that the inclusion of these items into the WA control list was done in good faith because of these reasons. Their inclusion represents a positive recognition that the unregulated sale of surveillance technologies by security vendors constitutes a risk to individual human rights and security.

The proposed rule has, however, caused widespread and serious concern among many sectors because of the potential inherent in it for unintended consequences, particularly the potential of language used within the new the proposed controls on items related to intrusion software to affect security research and the overall security of the internet. This is a concern that PI shares and we also recognise that there are limitations in respect of what the WA control list can achieve. Efforts to protect individual privacy, other human rights, and the security of modern networks, devices, and applications in the modern technological environment rely upon security research and international cooperation amongst researchers. Additionally, many of the technologies that may at first instance seem to be offensive in nature actually serve a vital component in building effective defensive capabilities for us all. The imposition of export licensing requirements therefore must only be upon strategically chosen, well-defined surveillance technologies, with explicit protections and exceptions for research.

It is our view that the US export control regulatory system and BIS's implementation of the items related to intrusion software require further clarification and safeguards. We strongly recommend that in order to fulfill the initial objectives of the controls an approach which takes into account the intent of the technology and software developer and by

incorporating end-use and end-user controls, and exceptions upon specific items. In addition, we recommend updating the WA dual use list language itself to clarify and provide certainty for all security researchers in the 41 states that adhere to the controls.

Given the need for further consultation, it is essential that another proposed final rule is published with clarifications and that another opportunity for public comment is provided, before a final rule is promulgated.

The remainder of this submission comprises the following sections:

1. **Why effective controls are a necessary and effective step**
2. **The proposed control of IP Network Surveillance Systems**
3. **The proposed control of items related to intrusion software**

1. Why effective controls are a necessary and effective step

The human rights impacts of surveillance exports are becoming increasingly evident: the private text messages of activists are read out to them as they are tortured; mass surveillance technology appears on the market, for purchase by repressive regimes that wish to monitor, collect and store the communications of entire populations; political refugees find their computers have been hacked and their digital life stolen. Surveillance technologies are used by governments to target opponents, journalists and lawyers, crack down on dissent, harass human rights defenders, intimidate populations, discourage whistle-blowers, chill expression and destroy the possibility of private life. In some cases, they also used to subject entire populations to indiscriminate monitoring. In short, they are often part of a broader state apparatus of oppression, facilitating a wide variety of human rights violations including unlawful interrogation practices, torture and extrajudicial executions.

The most obvious right affected by surveillance technology is the right to privacy, as any interception with communications or collection of personal data constitutes an interference with the right to privacy. Other rights that are frequently directly affected by surveillance include the right to freedom of expression and the right to freedom of association.

While subjecting specific surveillance technologies to export restrictions is not a silver bullet designed to comprehensively protect human rights, it is a necessary and major component of a comprehensive approach to ensuring that such items are not used for abuses and that states who assist in such abuses are exposed. Any strategy must also include the adoption of effective legal frameworks and systems of oversight within states using surveillance technologies, the widespread availability and adoption of encryption and anonymization technologies, and access to secure networks, devices, and applications. Importantly, even when they are not invoked to restrict a transfer of surveillance technology, export controls also act as an essential accountability and transparency mechanism.

It is therefore necessary and welcome that the new items were included within the 2013 WA control list. The WA also requires its members to regulate transfers of other surveillance technologies, such as mobile phone interception equipment known in the US as Stingrays, and laser microphones used to eavesdrop on conversations, for example through glass windows. It is important for the WA participating states to ensure that its control lists are up to date and appropriately control all surveillance technologies the trade of which represents a threat to the enjoyment of human rights.

While human rights are not considered a motivational factor for the decision to regulate the technology within Wassenaar, it is clear that the two states which instigated the inclusion of the new categories into the regime; France and the United Kingdom; were motivated at least in part by concerns relating to human rights.

2. The proposed control of IP Network Surveillance Systems

The category relating to IP Network Surveillance Systems in the WA was initiated by France after evidence emerged that a French company, Amesys, supplied internet backbone monitoring technology to Gaddafi's Libya. The Wall Street Journal reports that Amesys' Eagle monitoring system – a combination of probes using Deep Packet Inspection technology and analysis software – was "deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state" in Libya.[1] Amesys is facing an ongoing criminal case into its complicity in acts of torture by the Gaddafi regime.[2]

1Wall Street Journal, "Life Under the Gaze of Gadhafi's Spies" (14 December 2011), available at http://online.wsj.com/news/articles/SB10001424052970203764804577056230832805896.

2Business & Human Rights Resource Centre, "Amesys lawsuit (re Libya), available at http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496.

The IP Network Surveillance control goes a considerable way in subjecting many of the most prominent internet monitoring centers available on the market to control, including that of Amesys's product Eagle. As of 1 January 2015, the EU Dual-Use Regulation 429/ 2008 restricts the export of specialised large-scale IP monitoring systems, such as that sold by Amesys. France implemented the control almost immediately after it was approved by the WA in 2013.

i) Concerns

The requirement that the system must perform all of the listed functions, however, including relationship mapping, significantly narrows the range of products affected by the regulations. Carrying out analysis on "carrier class IP network" is aimed at targeting powerful analysis systems – specifically those that have the capacity to carry out large-scale analysis reliably. What constitutes "carrier class" is, however, open to interpretation, while there are a number of definitions that could be cited by competent bodies. "Analysis at the application layer" also greatly restricts the scope of the control, given that many surveillance products operate at layers other than the application layer.

Extraction of selected data and its indexing means that the product under restrictions needs to be actively retrieving the metadata and content from the IP traffic as well as actively storing this data.

Further, the controls call for the product to be "specially designed" to search through the captured data based on certain characteristics of an individual (such as name, political affiliation, etc) and must use be able to collate the captured data to identify relationships between the targeted individual or group.

ii) Recommendations

Privacy International believes that it is important that non-IP monitoring centres are also included within the WA control list, and recommends that the US government review export restrictions over such IP and non IP turnkey surveillance systems and brings them within national and WA control lists.

Regarding the implementation of ECCN 5A001j, we welcome the decision to designate the items as controlled for reasons of Regional Stability, which will mean that the items are assessed on a case-by-case basis and that promoting the observance of human rights will be a criteria used to assess applications. We strongly recommend that human rights implications are prioritised within the assessment process and that assessment criteria also includes:

- The compliance of the destination country with human rights obligations enshrined in the Charter of Fundamental Rights, the International Covenant on Civil and Political Rights, and other ratified instruments;
- The human rights record of the beneficial end-user authority, namely the agency or body proposing to purchase the technology, and;
- The existence or absence of an appropriate legal framework governing the use of the technology in the destination country, sufficient to ensure that the technology will be used in a manner compliant with human rights.

3. The proposed control of items related to intrusion software

The addition of items related to intrusion software were proposed by the United Kingdom and also agreed at the WA in December 2013. The following is a selection of PI's previous public comments on the topic:

- Announcement of controls on intrusion software and IP surveillance: https://privacyinternational.org/?q=node/398
- Export controls and implications for security research: https://privacyinternational.org/?q=node/354
- Open source software and export controls: https://www.privacyinternational.org/?q=node/344
- Our previous analysis of the US proposed rule: https://www.privacyinternational.org/?q=node/588

The targets of these additions to the dual-use list are items that have been popularly referred to by media as "state trojans", "lawful malware", or "spyware". They are marketed by security vendors for exclusive use by law enforcement and intelligence agencies as primarily useful for extracting data from a network-enabled device and for taking remote control of the device in order to actively monitor an individual target. The UK government has stated that these controls were targeted at "complex surveillance tools which enable unauthorised access to computer systems."[3]

The controls distinguished between components used to create and control the surveillance software and the software itself. For instance, such technology works by installing a Trojan on to networked devices and then using it to control functions such as the microphone or transmit data to a monitoring facility. The WA control does not target the Trojan component, but rather the command and control infrastructure used to generate, install and instruct the Trojan – i.e., the

3 https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

software installed on a government controlled server to deliver the Trojan to a target address. UK authorities have stated that this delineation was put in place to protect security researchers (i.e., those participating in sharing malware samples) and individuals infected by Trojans, given that any control on the Trojans themselves would put individuals carrying them on devices across borders under potential breaches of export regulations.

Subjecting such systems to export restrictions is necessary to protect human rights. The intrusive nature of this type of monitoring and intelligence gathering, the fact that it can be used against targets located anywhere in the world, and the absence of a clear and robust legislative framework governing their use makes these unlawful in their use. Widely-available evidence in the public domain shows how such products have been sold by companies and subsequently used for human rights violations.

High profile vendors of the targeted items based in the European Union, which implemented the controls within the Dual Use Regulation at the beginning of 2015, have indicated that their national export authorities have implemented the category into national law and are seeking export authorisation for their export.

Earlier this month, internal documents relating to Hacking Team, an Italian surveillance company, were leaked online. The documents showed that the company has customers listed in some 45 countries, including Azerbaijan, Bahrain, Colombia, Egypt, Ethiopia, Kazakhstan, Morocco, Oman, Russia, Saudi Arabia, Sudan, Turkey, UAE, and Uzbekistan. Hacking Team have a distributor in the US, Cicom, and have sold their technology to various US customers, including the Army, Federal Bureau of Investigations, and theDrugs Enforcement Agency. The documents also show that Hacking Team was not subject to export restrictions before the implementation of the new controls, and that they believe that they are now subject to individual license authorisation to export to countries outside of the WA.

Privacy International believes that this underlines both the necessity of subjecting the export of such systems to restrictions and license assessment criteria which prioritize human rights obligations.

i) Concerns

PI agrees with many of the general concerns already publicly advanced and submitted via this public comment process. In order to protect individual privacy and other human rights, and the security of the devices, networks and applications relied upon by everyone, including journalists, activists, and political opposition in authoritarian states, it is essential that implementation of the controls does not restrict security research. Subjecting specific security research tools and activities to restrictions, reporting requirements, and deemed exports provisions risks undermining the protection of privacy, as well as the commercial, foreign, and other interests of the US.

Privacy International's understanding from correspondence with the UK export control licensing authority was that the WA control was structured in a way to protect security research. These categories are not primarily intended to restrict exports of software vulnerability exploits, Proof of Concepts for such exploits, vulnerability research and non-public reporting of software vulnerabilities, training and international cooperation on how to identify and exploit vulnerabilities, commercial penetration testing software tools, fuzzers, or the presentation of research at international security conferences.

Privacy International believes that many of the above activities and items may not be subject to regulation by the proposed rule because they are either not defined within the scope of controls, because they are exempted as fundamental research, because they are ordinarily made publicly available, or because they are not “technology”. Nevertheless, we appreciate that the definitions of controlled items may subject critical security research activities and security research tools to regulation and impede or chill research activities that help protect network infrastructure and personal privacy interests.

For example, category 4e001c, technology required for the development of intrusion software, requires greater clarity and more effective implementation. This category would control exploit “technology”, defined as technical data (blue prints, design plans) or technical assistance (training), if it is for the “development” of software “specially designed” to avoid protective measures (anti-virus software) and extract or modify data or modifying the standard execution path of software in order to allow the execution of externally provided instructions, and if the export is not subject to an “publicly available technology and software” exception. The fact that a controlled item needs to be “technology” “required” for the “development” of intrusion software and that software needs to be “specially designed” and “peculiarly responsible” to fulfill all of the functions considerably narrows the scope of products subject to licensing. The proposed rule would not control technology simply for discovering or identifying vulnerabilities, or testing the vulnerability to determine what happens. We also acknowledge the realities of many security processes such that much of the research conducted will never become publicly available and therefore, the publicly available exception is not adequate.

This would mean, however, that if an individual were to, for example, draw up a design plan of how to develop an

exploit “specially designed” to carry out of these functions, and were to “export” it to a foreign company or to a non-US national, then they would require a license. This has implications for individuals and companies involved in research cooperation. Given the publicly available exception and protections for fundamental research, this would primarily affect independent researchers and those in the private sector who need to be able to collaborate, often across borders or with non-US nationals. Employees within the same company would not be exempted under the current language. Often, security researchers are not affiliated with an academic institution, and have no control over whether such “technology” is ever made publicly available. Indeed, in some cases, it is undesirable for the “technology” to be made publicly available, given that it is then made available for attack. It also has implications for companies involved in specialised training. If a company was providing training for profit on how to develop that particular type of exploit, they would need a license. They would also need one for training non-US individuals.

The control on the “software,” “systems,” “equipment,” or “components” “specially designed” for the generation, operation or delivery of, or communication with, “intrusion software” will regulate some essential security research equipment. For example, commercial penetration testing tools that are not open source and that are considered “specially designed”, require a license for export.

To a large extent this is because of the decision in the proposed rule not to implement the first paragraph of the Wassenaar Software Note. Although the open source exception applies, the “mass market” exception – anything generally available to the public through normal points of sale – does not apply to any of the categories. We understand that the basis for this decision is that most items identified as potentially controlled were already controlled because of the controlled encrypted functionality within them and were therefore already not eligible for exemption. However, this is extremely problematic. UK authorities noted to Privacy International that the WA General Software provides additional protections for the security research community, because they believed that software targeted at the penetration testing community is almost exclusively open source or commercially available without restriction and thus not subject to this export control because of the General Software Note (GSN). While the GSN provides essential protections however, it is not sufficient to take into account the realities of how security research is conducted and accordingly we are calling for additional safeguards to be expressly stated in the text of any regulation.

Some security research tools will not be subjected to restrictions because they are not considered to be “specially designed” to carry out the functions in the controlled categories. Nevertheless, as a notoriously complex area of export control law to understand, this will chill security research and the development of security tools by small and medium enterprises and individuals not familiar with export regulations, even if they are not in fact subject to any restrictions. It is vital that any regulation be clearly and concisely stated in writing and in the actual text of the regulation itself – Privacy International does not consider any FAQs or telephone calls to be sufficiently authoritative in respect of this issue.

Deemed Exports regulations will further amplify the negative consequences of implementing the proposed rule in its current form. While there are exceptions protecting research and the dissemination of research at public conferences, this will most obviously have negative implications for research cooperation, training on use of controlled security research tools, and the provision of specialised training on how to develop “intrusion software” to customers abroad or to non-US citizens in the US.

ii) Recommendations

All of the categories related to intrusion software require greater clarity and more effective implementation. Privacy International recommends that additional exceptions be applied to the categories and that specific activities and items are clearly excluded from control in any final rule. As a result of the confusion and concerns caused by the new categories, we also strongly recommend that a new proposed final rule is published and that another round of public comments is made available.

We recommend that additional exclusions are included to narrow the scope of the new licensing requirements to only apply if the exporter is aware that the export may be intended for ultimate end-use by a government end-user for the monitoring of IP network enabled-devices for intelligence gathering or law enforcement purposes. While this approach suffers from enforcement difficulties, it is nevertheless still an effective means by virtue of the fact that the vast majority of surveillance technology manufacturers explicitly and exclusively sell their products to government end-users for the purposes of surveillance. We also recommend that additional exclusions are put in place to consider the purpose and motivation for the work. For example, it would not be appropriate to restrict a researcher sending a PoC to a government agency regarding a vulnerability in its website or other software system.

A precedent for this approach exists within the CIV exception. For example, for certain items on the CCL list that usually require a license for export to the ultimate destination, the CIV exception allows items to be exported to civil-end users for civil end-uses in selected countries. This license exception is available if the item is controlled only for national security (NS) reasons. Such an exception applied to the categories related to intrusion software would therefore

only regulate the export of "technology" or systems if they are intended to be used for surveillance by government end-users, and would avoid placing regulatory burdens upon security research not intended to be used in that area.

Further exceptions should also be applied in order to clarify what activities and items are explicitly not subject to restrictions to stop the chilling effect of any complex regulations. We recommend that any security research items and activities subject to restrictions that BIS is aware of and that have been brought to its intention via this public comment process be explicitly excluded from licensing requirements within the rule itself, even if they are already excluded by the general exceptions or are not subject to restrictions in the first place. Such items and activities include, but are not limited to, software vulnerability exploits, Proof of Concepts for such exploits, vulnerability research and non-public reporting of software vulnerabilities, training and international cooperation on how to identify and exploit vulnerabilities, commercial penetration testing software tools, fuzzers, and the presentation of research at international security conferences.The research on any of these must also be protected, whether it is publicly available or not.

A precedent for this approach exists within the APP exception. This exception enables exports of computers and associated technology and software of certain "Adjusted Peak Performance" (APP) levels to certain groups of countries, provided there is no evidence of intention for certain end uses. Such an exception can be used in relation to the new categories to explicitly exclude specific technology from control.

We also recommend that the mass-market exception within the GSN be reinstated.

We welcome the decision to designate the items related to intrusion software as controlled for reasons of Regional Stability, which will mean that the items are assessed on a case-by-case basis and that promoting the observance of human rights will be a criteria used to assess applications. We strongly recommend that human rights implications are prioritised within the assessment process and that assessment criteria also includes:

- The compliance of the destination country with human rights obligations enshrined in the Charter of Fundamental Rights, the International Covenant on Civil and Political Rights, and other ratified instruments;
- The human rights record of the beneficial end-user authority, namely the agency or body proposing to purchase the technology, and;
- The existence or absence of an appropriate legal framework governing the use of the technology in the destination country, sufficient to ensure that the technology will be used in a manner compliant with human rights.

Privacy International thanks BIS for their attention in this matter and is available for further consultation on any of the issues discussed above.