June 2, 2020

To:

The Business & Human Rights Resource Centre

Re: Your Request for Response Dated May 29, 2020

Dear Sirs/Madams,

In response to your request for a response referenced above, we would be pleased to provide the following response.

NSO develops and licenses to States and State agencies technologies intended to thwart serious criminal acts that threaten life, liberty, safety, and personal security. NSO offers its technology to verified and authorized government agencies for national security and law enforcement purposes, to meet the challenges of encryption used by terrorists and criminals. In many cases, traditional intelligence-gathering tools used by government agencies to prevent terrorism and serious crime are no longer effective. NSO's technology is designed to lawfully intercept communications for the sole purpose of preventing or investigating serious crimes and terrorism. The use of NSO's technology has contributed to prevent terror attacks, stop human trafficking cartels, break up child exploitation rings, and bring home kidnapped children. But we are aware that our products, as for any other company, can be misused. This is why NSO has been developing its Human Rights Program for the implementation of the UN Guiding Principles on Business and Human Rights (UNGPs) and is committed to being transparent in its approach. In this spirit, we welcome the opportunity to provide further details on our approach and policies.

First, sales and exports of our Pegasus technology are strictly monitored and regulated by the Government of Israel. The export of the technology is regulated under Israel's Defense Export Control Law and each such export requires a specific license from the Israel Ministry of Defense (IMoD). These licenses provide restrictions on potential customers and engagements, as well as permitted uses. As a condition under these license NSO is required to provide the IMoD with signed certificates from the end-users of NSO's Pegasus technology in which the end-users declare that NSO's Pegasus technology will be used only for prevention and investigation of terrorism and criminal activity.

NSO does not operate the products itself, or on behalf of our customers. NSO's role is limited to the provision of technical support and maintenance services for its customers. NSO government customers operate the Pegasus technology themselves, to advance their own interests of fighting terrorism and serious crime. But NSO requires, as a condition of use, that its government customers agree that they (1) will use NSO's Pegasus technology "only for the prevention or investigation of crimes and terrorism and ensure that the [technology] will not be used for human rights violations" and (2) will immediately notify NSO of any potential misuse. NSO can contractually suspend or terminate service to customers engaged

NSO Group Technologies LTD I22 Galgalei HaPlada St. P.O.B 4166, Hertsliya, 4672222, Israel I
Telephone: +972.77.4341292 I Fax: +972.77.4253513 I I Email: office@nsogroup.com

in any improper use of its Pegasus technology outside these parameters. (See Compl. Exh. 11, Sec. 7.) and has done so in the past.

NSO's Pegasus technology also has technical safeguards, such as general and customer-specific geographic limitations, including that NSO's Pegasus technology cannot be used by foreign governments against U.S. mobile phone numbers or against a device within the geographic bounds of the United States.

More broadly, NSO is committed to lead its industry in taking governance extremely seriously, and in its commitment to ethical business; as demonstrated by the rigorous standards the company has in place for conducting human rights due diligence and vetting potential end users to assure proper use of its systems. The policies and procedures that help shape the program are designed to mitigate the risk that NSO is directly linked to unlawful and arbitrary interference with rights to privacy, or infringements of freedom of expression, by the users of its products. In late 2019, NSO further strengthened its compliance system, which included instituting an enhanced governance framework, to further mitigate the risks of possible adverse human rights impacts. Every contract with a government or law enforcement agency needs to meet both legal requirements and NSO's approval process to ensure the technology is used as designed. NSO has established a Governance, Risk and Compliance Committee of the Board of Directors, which is responsible for public disclosures, in consultation with experienced external advisers and human rights experts. This Committee also provides oversight on the full implementation of these Human Rights Policies.

NSO also recently adopted an upgraded human rights due diligence procedure that applies to all future engagements and renewals. Under the procedure, when a new opportunity arises, which can range from a general possibility to engage with a State or State agency, NSO conducts a human rights-focused country-level assessment. This includes the prospective country's human rights record, as well as its perceived respect for the rule of law and freedom of speech, political stability, and level of corruption. That analysis relies on a number of authoritative public indicators, such as the World Bank Worldwide Governance Indicators and the Transparency International Corruption Perception Index. At this initial stage of review, NSO also considers the nature of its product and its potential for misuse – as NSO has a wide portfolio of products with varying potential risks of misuse – NSO's prior relationship with the entity that will use its products, the credibility of that entity and its defined mission, the duration of potential use, and other factors which could potentially increase or decrease human rights risks.

At the conclusion of this initial stage of review, NSO's compliance team categorizes the opportunity according to the risks of potential negative human rights impacts. As a rule, NSO does not pursue opportunities where the human rights risks are unduly high, and thus the process could stop here. If the process does proceed, NSO conducts additional diligence steps. The specific steps taken differ depending on the level and nature of potential risk, but they generally include a review by an external risk and investigation firm, an assessment of adverse public information, and a detailed analysis of the domestic legal framework. Among the legal issues analyzed are whether domestic standards and protections are consistent with International Covenant on Civil and Political Rights Articles 17 and 19, including the accessibility of the law, the clarity of the law, the foreseeability of the impact, and other essential factors identified by human rights courts and tribunals. In addition, at this point of the process, further information might be obtained directly from the anticipated user, depending on the nature of the situation and the potential risks identified. When that information has been accumulated, NSO may consult with

external experts and advisors to determine the appropriate course of action. That includes potential measures that reasonably may be employed to prevent and mitigate the risks of misuse and negative impacts if the engagement proceeds. If the risks, even with mitigating measures, are deemed unduly high, NSO will terminate discussions and the engagement will not proceed.

If the engagement proceeds, NSO's contracts will include, at a minimum, detailed Human Rights provisions that are consistent with NSO's Human Rights Policy, an ability to suspend NSO's systems upon suspected misuse, and an agreement to cooperate in any investigation into potential misuse. These provisions help provide confidence that, regardless of the domestic framework, users are abiding by our standards, which are consistent with human rights norms. NSO also may seek additional remediation measures, such as representations and warranties from users, insist on a shortened contract duration, request that users undergo human rights training, and other steps. Our systems are also configured in a manner that limits the use by our customers, to a specified duration, to a limited number of concurrent targets, and in specific regions, to minimize risks of misuse.

Finally, NSO monitors and reviews all entities that use its technologies both on an ongoing and periodic basis. This may include engagement with NSO's customer or user representatives, media searches for adverse information, updated reviews of due diligence reports, meetings with the end-user personnel, and in-country visits by NSO's legal and compliance team.

NSO takes several steps in instances where NSO's technologies as suspected of being used in a manner inconsistent with domestic law, international norms, or the contract. NSO generally suspends use of the technology and investigates the potential misuse. It also may obtain further legal advice, consult with external experts, and pursue additional efforts.

Where misuse is identified, NSO generally suspends use of the technology and investigates the potential misuse. It also generally will seek to use the leverage it might possess – consistent with the UNGPs 13, 19 and 22 – to take appropriate action to prevent or mitigate any adverse human rights impacts. That may include insisting on periodic certifications and declarations prior to maintenance renewals, instituting further product restrictions based on volume and geographic coverage, conducting a review of operational security, requiring users to participate in enhanced training, and other tailored measures. For instance, in recent instances in which NSO has received concerns or complaints regarding alleged misuse, it has immediately stopped the customer's use of the system, conducted a detailed review of the domestic legal frameworks, reviewed the relevant contracts and agreements, interviewed the users and their legal representatives to understand their processes, protections and perspectives, and verified facts from objective sources. NSO has reinstated the system only after gaining comfort that the system was not misused. As mentioned above, NSO has terminated contracts in multiple instances and severed relationships with customers after misuses were identified, and will terminate agreements if the user does not cooperate in our inquiries.

NSO is proud to be the first company in the cyber industry that is implementing policies towards complete alignment with the United Nations Guiding Principles on Business and Human Rights. We work on a constant basis to improve our policies and practices to further assure that no misuse is committed in the use of our systems, particularly given the absence of best practices and guidance both for States to

appropriately balance their essential law enforcement and crime prevention efforts with their human rights obligations and for our industry's responsibility to respect privacy and other human rights.

NSO thus welcomes this opportunity to respond to your esteemed Centre in these regards. We hope this clarification helps shed light on our evolving program. As we have noted, we are continuing to refine our approach, and we would welcome further constructive dialogue from all stakeholders to respond to the challenges of the technology and human rights nexus.

NSO Group Technologies LTD I22 Galgalei HaPlada St. P.O.B 4166, Hertsliya, 4672222, Israel I
Telephone: +972.77.4341292 I Fax: +972.77.4253513 I I Email: office@nsogroup.com