Hogan Lovells

State Department signals increased focus on surveillance technology and human rights abuses

10 September 2019

On 4 September 2019 the U.S. State Department issued "Draft 'U.S. Government Guidance for the Export of Hardware, Software and Technology with Surveillance Capabilities and/or parts/know-how'" (draft guidance). Although the draft guidance does not specify any particular government's use of surveillance technology, the release of this document is consistent with the Trump administration's recent focus on the use of surveillance by certain governments against civilian populations in trouble spots around the world. This guidance is not mandatory for export control and sanctions compliance purposes, but it is relevant for companies to consider in building and enhancing their compliance programs.

The State Department's draft guidance reflects an increased focus by the U.S. government on human rights concerns and entities that aid governments in the restriction of human rights and individual expression. Specifically, the draft guidance focuses on the export of items that "can be misused to violate or abuse human rights when exported to government end users or private end users that have close relationships with the government." The State Department notes that the use of surveillance hardware, software, and technology by governments around the world "to subject entire populations to arbitrary or unlawful surveillance" is of particular concern. As such, the draft guidance highlights due diligence considerations that all exporters should take into account when dealing in items with "intended and unintended surveillance capabilities" and urges exporters to "integrate human rights due diligence into export control compliance programs."

Notably, the draft guidance does not apply to just makers of items designed for surveillance, such as cameras or listening devices, but has much broader implications. For example, companies involved in software development, big data, social media, telecommunications, artificial intelligence, facial recognition, natural language processing, or other fields that could have unintended surveillance capabilities need to consider not just the intended uses of their products, but how parties could misuse their products to engage in human rights abuses or suppress free expression.

Companies have until 4 October 2019 to provide the State Department with feedback and comments; after that date, the State Department will remove the draft guidance from its website and work to finalize the draft.

While this guidance is not comprehensive or mandatory under U.S. law, it is illustrative of the approach that the State Department and other agencies or departments of the U.S. government (e.g., the U.S. Commerce Department's Bureau of Industry and Security (BIS) and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)) may take toward companies that export hardware, software, or technology with surveillance capabilities. In particular, this guidance could be used to assess the need to impose secondary sanctions under U.S. sanctions programs that target human rights abuses either under the Global Magnitsky Executive Order (which has a global reach) or under specific country programs (e.g., Venezuela, Nicaragua, the Democratic Republic of the Congo).

The draft guidance can be understood as a set of "best practices" that companies operating in this space should use to benchmark their own policies and procedures against the U.S. government's expectations for exporters of sensitive technologies that are susceptible to misuse in the wrong hands, and as a roadmap for steps that companies can take to mitigate these risks.

Items with intended or unintended surveillance capabilities

The draft guidance takes a broad approach to items covered and includes "hardware, software, technology, technical assistance, services, and/or parts/know-how that is marketed for or can be used for the monitoring, interception, collection, preservation and/or retention of information that has been communicated, relayed or generated over communications networks to a recipient or group of recipients" with intended or unintended surveillance capabilities. Examples provided by the State Department of such items include the following:

- Spyware
- Crypto-analysis products
- Penetration-testing tools
- Information technology products with deep packet inspection functions
- Specialized computer vision chips
- Noncooperative location tracking (products that can be used for ongoing tracking of individuals' locations without their knowledge and consent)
- Cell site simulators (Stingrays)
- Automatic license plate readers
- Body-worn cameras
- Drones and unmanned aerial vehicles
- Facial recognition software; thermal imaging systems
- Rapid DNA testing; automated biometric systems
- Social media analytics software; gait analysis software
- Network protocols surveillance systems
- Devices that record audio and video and can remotely transmit or can be remotely accessed

Characteristics of due diligence

The draft guidance takes a broad approach to what is considered appropriate "due diligence" that exporters should undertake, including:

- Assess and address risk: The level of due diligence and how much due diligence to conduct should be commensurate with the severity and likelihood of an adverse impact, where more significant risks are prioritized.
- Ongoing assessment of monitoring and evaluation: Ongoing, responsive, and changing process that includes monitoring, evaluation, and feedback loops to verify whether adverse impacts are being effectively addressed and new potential impacts identified.
- Stakeholder engagement: Ongoing communication with those whose interests could be affected by the exporter's activities.
- Public communication: Communication of the exporter's commitment to a rigorous internal and external review of human rights risks and to adequate measures to address these risks.
- Alignment with human rights instruments: Review process should be based on the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), the Organisation for Economic Co-operation and Development Guidelines for Multinational Enterprises, and the United Nations Guiding Principles on Business and Human Rights.

Such due diligence considerations should be widely integrated into export control compliance programs, including "support from the highest levels within an exporter's organization, training on relevant human rights considerations for employees, documentation, and communication of both commitment and steps taken in this regard."

Human rights due diligence and risk mitigation considerations

The State Department has offered the following general guidance for exporters to ensure compliance with applicable human rights laws[1]:

1. In general, tailor the item to minimize the likelihood that it will be misused to commit human rights violations or abuses.
2. Review the capabilities of the export in question to determine potential for misuse to commit human rights violations or abuses by government end users and private end users that have close relationships with a foreign government.
3. Review the human rights record of the government agency end user of the country intended to receive the export.
4. Review whether the government end user's laws, regulations, and practices that implicate items with surveillance capabilities are consistent with the ICCPR. (Relevant resources are provided by the State Department in the two appendices that accompany the draft guidance).
5. Review stakeholder entities involved in the transaction (including end users and intermediaries such as distributors and resellers). Refer to BIS "Know Your Customer Guidance."
6. Strive to mitigate human rights risks through contractual and procedural safeguards, and strong grievance mechanisms.

[1] The draft guidance also contains "due diligence considerations," transaction "red flags," and other situation-specific guidance that may be of use to exporting entities depending upon their industry.

7. After export, strive to mitigate human rights risks through contractual and procedural safeguards, and strong grievance mechanisms.

8. Publicly report on the export transaction (e.g., in annual reports or on websites).

Trends and other steps for consideration

As noted above, the draft guidance is not "comprehensive or mandatory" under U.S. law, though it may be indicative of the approach that certain agencies and departments within the U.S. government may take toward surveillance items that are connected to various government human rights abuses. While the draft guidance could have far-reaching impact throughout the U.S. government, exporters should be particularly mindful of the following possibilities:

- Possible increased use of secondary sanctions: As noted above, the State Department's focus on items that could be used to "violate or abuse human rights" could signal an intent by the U.S. government to increase enforcement measures – including the use of secondary sanctions – against companies found to be aiding governments restricting or abusing human rights.

- Possible increased scrutiny of state-owned enterprises (SOEs): The draft guidance also signals that SOEs operating within certain countries could come under greater scrutiny. Specifically, the draft guidance identifies at least two red flags that could relate to SOEs:

    1. The end user is not a government, but has a close relationship with a government that has a reputation for committing human rights abuses or violations, and in particular the kinds of human rights violations or abuses the exported item could help facilitate.

    2. The stated end user in the export transaction is likely not the only end user.

- Possible increase scrutiny of the design of surveillance items: The draft guidance indicates that exporters should be mindful of the "design" of certain items and should tailor the items to "minimize the likelihood that it will be misused to commit human rights violations or abuses." These statements indicate that agencies and departments within the U.S. government may begin to more closely examine the actual design of exported surveillance items, which could place additional pressure on exporters to conduct higher levels of due diligence on the end user and potential end uses of surveillance items.

As such, exporters may consider taking the following steps:

- Distribute this draft guidance to appropriate personnel, particularly those in certain high-risk regions susceptible to secondary sanctions such as Venezuela, Russia, and the Middle East.

- Consider incorporating relevant human rights considerations into standard employee trade compliance training.

- Carefully evaluate any ongoing projects that could be found to involve surveillance items, especially with SOE and government end users that have been accused of human rights abuses.

- In new contracts and engagement letters, consider incorporating language that references the exporter's commitment to preventing human rights abuses.

For further information or assistance, please contact any of the Hogan Lovells lawyers identified below.

Contacts

Aleksandar Dukic
Partner, Washington, D.C.
T +1 202 637 5466
aleksandar.dukic@hoganlovells.com

H. Deen Kaplan
Partner, Washington, D.C.
T +1 202 637 5799
deen.kaplan@hoganlovells.com

Warren H. Maruyama
Partner, Washington, D.C.
T +1 202 637 5716
warren.maruyama@hoganlovells.com

Beth Peters
Partner, Washington, D.C.
T +1 202 637 5837
beth.peters@hoganlovells.com

Jared R. Wessel
Counsel, Washington, D.C.
T +1 202 637 6472
jared.wessel@hoganlovells.com

Adam J. Berry
Senior Associate, Washington, D.C.
T +1 202 637 2871
adam.berry@hoganlovells.com

Ari Fridman
Senior Associate, Washington, D.C.
T +1 202 637 5449
ari.fridman@hoganlovells.com

Chris R. Mullen
Associate, Washington, D.C.
T +1 202 637 6687
chris.mullen@hoganlovells.com

www.hoganlovells.com