# DRAFT U.S. GOVERNMENT GUIDANCE FOR THE EXPORT OF HARDWARE, SOFTWARE AND TECHNOLOGY WITH SURVEILLANCE CAPABILITIES AND/OR PARTS/KNOW-HOW

Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

- UN Guiding Principles on Business and Human Rights

Items with intended and unintended surveillance capabilities ("item(s)") have the vast potential to provide positive contributions to a country's economic, defense, and societal wellbeing. These items can be a force multiplier in providing solutions to urgent policy challenges facing society. Such items promise to reshape healthcare and manufacturing, among others sectors, around the world.

At the same time, these items 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. In some cases, governments have misused these items to subject entire populations to arbitrary or unlawful surveillance, violating the right to privacy as set out in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). In other cases, governments employ these items as part of a broader state apparatus of oppression that violates human rights and fundamental freedoms enumerated in the UDHR and ICCPR, including freedoms of expression, religion or belief, association and peaceful assembly.

The misuse of an item can take many forms, including to stifle dissent; harass human rights defenders; intimidate minority communities; discourage whistle-blowers; chill free expression; target political opponents, journalists, and lawyers; or interfere arbitrarily or unlawfully with privacy. Arbitrary or unlawful interference with privacy is a particular concern in this context, especially since such interference may also impede the enjoyment of other human rights, such as the rights to freedom of expression, to hold opinions without interference, and to freedom of association and peaceful assembly. These and other rights are among the foundations of any democratic society.

#### **Purpose:**

This guidance seeks to assist exporters of items with intended and unintended surveillance capabilities with implementation of the UN Guiding Principles on Business and Human Rights (UNGPs) as well as the OECD Guidelines for Multinational Enterprises (Guidelines). The guidance aims to provide insight to exporters on considerations to weigh prior to exporting these items. It also offers businesses greater understanding of the human rights concerns the U.S. government may have with the export. Appendix 1 provides a list of recommended resources that businesses may find helpful to consult when conducting due diligence on the export of items with intended and unintended surveillance capabilities. For global context, Appendix 2 provides

<u>DRAFT</u>

a list of general issues of human rights concern that have arisen related to such items, including examples of relevant government laws, regulations and practices.

The United States government is committed to the promotion and protection of human rights. In that spirit, the exporter of an item should carefully review this guidance, and consider whether to participate in, or continue to participate in, an export transaction if the exporter identifies a risk that the end-user will likely misuse the item to carry out human rights violations or abuses. Exporters are encouraged to integrate human rights due diligence into export control compliance programs. Such integration should include 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.

This guidance is not intended to be, nor should it be interpreted as, comprehensive or mandatory. The Department of Commerce's Bureau of Industry and Security (BIS) and the State Department's Directorate of Defense Trade Controls (DDTC) are responsible for regulating the export of many types of dual-use items, defense articles and defense services, respectively. BIS maintains a set of Red Flag Indicators and "Know Your Customer Guidance" for exporters to follow when exporting items subject to the Export Administration Regulations. This guidance is also not meant to address any requirements under export control laws. Exporters are responsible for obtaining appropriate licenses and/or approvals for the export of controlled dual-use items, defense articles and defense services.

### **Definitions:**

**Due Diligence:** For the purpose of this document, "due diligence" is defined as the process by which an exporter works to identify, anticipate, prevent, mitigate, and account for how it addresses actual or potential adverse impacts on human rights of individuals. This includes impacts that it may cause or contributes to, or to which it is otherwise directly linked. Due diligence is an integral part of business decision-making and risk management systems.

Characteristics of due diligence include but are not limited to:

- 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, the OECD Guidelines for Multinational Enterprises, and the UN Guiding Principles on Business and Human Rights.

**Legitimate Law Enforcement Purpose:** For the purpose of this document, "legitimate law enforcement purpose" means use by law enforcement, including government agency providing security services, consistent with state commitments to the Universal Declaration of Human Rights.

**Red Flag:** For the purpose of this document, a "red flag" is any information that arises through any source where follow-up, assessment, and/or further due diligence is warranted. Not all red flags carry equal weight – rather, it depends on the context and surrounding circumstances. The mere existence of a red flag does not mean that an action or transaction should be terminated, but rather that it should be evaluated in the context of other red flags and context-specific factors. This document does not provide an exhaustive list of red flags.

Item with Intended or Unintended Surveillance Capabilities: For the purpose of this document, "item with intended or unintended surveillance capabilities" [also referred to as "item(s)" in this document] 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.

Items covered by this guidance ranges from consumer-grade to dual-use items listed on the Commerce Control List and defense articles and defense services listed in the International Traffic in Arms Regulations. Examples of items with surveillance capabilities, include, but are not limited to: spyware; crypto-analysis products; penetration-testing tools; information technology products with deep packet inspection functions; specialized computer vision chips; non-cooperative 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; and devices that record audio and video and can remotely transmit or can be remotely accessed.

## **Human Rights Due Diligence and Risk Mitigation Considerations:**

- 1. In general, tailor the item to minimize the likelihood that it will be misused to commit human rights violations or abuses.
  - Integrate safety and 'privacy by design' features that:
    - enable tracking of deployment;

- alert the exporter to misuse;
- enable the exporter to strip certain capabilities from the item prior to export;
- o limit the use once sold;
- o provide a kill switch;
- o limit upgrades, software updates, and direct support;
- o provide for data minimization;
- o auto deletes data.
- 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.

## Due Diligence Considerations:

Review item and conduct assessments to determine if such item could be misused
to violate or abuse human rights, including the rights to freedom of expression,
peaceful assembly, freedom of association, and the right to be free from arbitrary
or unlawful interference with privacy.

#### Red Flags:

- Information (e.g. reports, articles, publications) that indicates similar item has been misused to commit human rights violations or abuses;
- The export includes item that could be used to build, customize, configure, or integrate a system that is known to be misused to commit human rights violations or abuses or it is likely that it will be.
- 3. Review the human rights record of the government agency end-user of the country intended to receive the export.

### **Due Diligence Considerations:**

- Review credible reports of the human rights record of the recipient government agency end-user, including the <u>U.S. Department of State's annual Human Rights Report</u>, news reports, and information from non-governmental and/or local sources. Reviews should focus on the specific entity within the government, as feasible. See Appendix 1 for additional recommended sources and Appendix 2 for general examples of laws, regulations, and practices that have raised human rights concerns;
- Reach out to non-governmental organizations (globally and on the ground) to access first-hand knowledge of the human rights record of the recipient government agency end-user. See Appendix 1 for a list of some organizations to engage;
- Consider whether the government agency has used technology to target individuals in retaliation for the exercise of their human rights or on

- discriminatory grounds prohibited by international law (e.g. journalists or members of religious minority groups);
- Consider the nature of the relationship between the importing government agency and the part of the government that provides security services;
- In cases where the government agency end-user is a provider of security services, consider whether there are instances where item has been misused, for something other than a legitimate law enforcement purpose.

#### Red Flags:

- Information regarding government agency end-user's misuse of the item to commit human rights violations or abuses (e.g. reports, articles);
- Laws, regulations, or government practices that unduly restrict civic space and/or target individuals or members of a group solely on the basis of their race, sex, language, religion, political opinion, national origin, or any other grounds inconsistent with international human rights law;
- Ongoing conflict or political turmoil in region being exported to;
- Ongoing abuse or arbitrary detention of members of minority groups, civil society members, or journalists (e.g. for exercising freedom of expression);
- Lack of independent judicial oversight/rule of law;
- Government agency end-user provides security services and has misused the item for something other than a legitimate law enforcement purpose;
- Government agency end-user has a close relationship with the part of the government that provides security services and that part of the government has misused the item to commit human rights violations or abuses;
- Government end-user has a record of human rights violations or abuses, including where a government end-user's record on human rights is so poor that it raises credible concerns that the exported item would be misused to facilitate governmental human rights violations or abuses;
- Government purchases the item from other governments with poor human rights records or from private actors with a history of unsavory exports to such governments;
- Government end-user has a history of exporting items to other countries with authoritarian governments and history of committing human rights violations or abuses.
- 4. Review whether the government end-user's laws, regulations, and practices that implicate items with surveillance capabilities are consistent with the ICCPR. See Appendices 1 and 2.

#### Due Diligence Considerations:

• Review laws, regulations, or practices that may unduly hinder freedom of expression, and/or interfere unlawfully or arbitrarily with privacy, as feasible;

- Review laws, regulations, or practices concerning government interception of private communications, and government access to stored private communications, as feasible;
- Review the extent to which the government implements its laws on surveillance and the oversight mechanisms in place, as feasible;
- Review the IT infrastructure of the export destination country to determine level of government access and/or control, as feasible.

#### Red Flags:

- Laws (pending or otherwise) or practices that provide for government access to information and communications technology company data without reasonable safeguards and appropriate oversight;
- Laws, regulations, particularly counterterrorism or national security-related laws or regulations, or practices that appear to unduly restrict freedom of expression or interfere unlawfully or arbitrarily with privacy;
- Government's engagement in malicious cyber activities against individuals or dissident groups;
- Lack of independent judicial oversight/rule of law;
- Data-sharing with governments with poor human rights records or data localization requirements;
- Total or significant government control or ownership of IT infrastructure and/or Internet Service Providers or telecommunication networks beyond that used for its own systems and communications (e.g., partially state-owned enterprise). See Appendix 2 for examples.
- 5. Review stakeholder entities involved in the transaction (including end-user and intermediaries such as distributors and resellers). Refer to BIS <u>"Know Your Customer Guidance"</u>.

#### **Due Diligence Considerations:**

- Review how the intermediaries and/or end-users intend to use the item, before and during any transaction;
- Review or seek to ascertain whether the end-user is intending to or likely to contract the work involving the item in question to non-governmental entities or individuals, including possible foreign nationals, inside or outside the receiving country;
- If the end-user is not the government but has a close relationship with a government, review the level of control the government has over the entity in question. If the government has strong ties to the entity in question and the government has a record of committing human rights violations or abuses, considerations 3-4 above may still be relevant;
- Review risks that the item will be transferred or diverted to a different end-user from the one listed on the license application;

• Review, to the extent possible, the end-user government's history, if any, of use of the type of item associated with the export.

## Red Flags:

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

# 6. Strive to mitigate human rights risks through contractual and procedural safeguards, and strong grievance mechanisms.

# Contractual and Procedural Safeguards

- Include human rights safeguards language in contracts. The language should be specific to human rights risks identified and/or associated with the item;
- Include protections for the exporter in the contract: export compliance clauses
  requiring end-users to agree to comply with applicable U.S. export control laws
  and regulations; limitations on how the item can/cannot be used; how and by
  whom collected data is to be analyzed, stored, protected, and shared; and reserve
  the exporter's right to terminate access to technology, deny software updates,
  training, and other services and/or unilaterally terminate the contract if the
  exporter uncovers (in its sole discretion) evidence that the technology is being
  misused;
- Adopt access and distribution mechanisms and contractual provisions that authorize the exporter to maintain full control and custody of the item and terminate access if necessary to minimize risk of diversion (e.g., Application Program Interface (API) access rather than on-premises installations; license keys requiring periodic renewal rather than permanent activation);
- Establish a preventative framework to address possible cases of license revocation. (e.g., the exporter may stop providing support, updates, and training or cut off the licensees' access to any cloud-based portion of the service at any time);
- Provide routine human rights due diligence training to all employees involved in the transaction.

## **Grievance Mechanisms**

- Develop secure, accessible, and responsive communications channels for both internal and external actors to report possible misuse of an export (e.g. reporting mechanism through company website);
- Develop procedure to ensure those reporting a misuse of an export are protected from retaliation:

- Exporter should have a formal follow-up mechanism, including an investigation and feedback loop to the actor reporting misuse;
- Exporter should regularly review and update communication channel to make sure it is effective.

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

## Contractual and Procedural Safeguards

- Invoke contractual protections that permit the exporter to immediately stop providing upgrades, direct support, and other assistance in the event of breaches of contractual terms and conditions;
- Reassess human rights due diligence considerations prior to license renewal; new activities, provision of services to, or relationships with the customer; major changes in the business relationships; and social and political changes in the country where the customer resides;
- Stay aware of news developments and shifts in a customer's home country in
  order to stay abreast of how the item could be used by the government to restrict
  civic space and/or target journalists, vulnerable groups or minority groups (e.g.,
  reach out to civil society groups on the ground and locally, carry out on-going
  due diligence after sale).

## **Grievance Mechanisms**

- Quickly and thoroughly investigate all complaints of misuse. Remotely disable
  the item, and limit upgrades and customer support when a credible complaint of
  misuse is received, until investigation is complete;
- Where misuse is found, follow-up with actor filing report to provide remedy where possible.

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

- At least annually, publicly report on human rights due diligence (e.g. steps taken to prevent human rights violations and abuses; data requests; evidence of misuse and steps taken to redress the harm);
- At least annually, publicly report on how credible complaints raised through communication channels were resolved (e.g., high-level summary).
- Publish a human rights policy;
- Publicly reporting on a website, in a public annual report, or an otherwise accessible location.

# Appendix 1 – Human Rights Tools, Reports and Guidance

<b>Information Source or Tool</b>	Description	
U.S. Government Information and Tools		
U.S. Department of State Human Rights Report	The annual Country Reports on Human Rights Practices – the Human Rights Reports – cover internationally recognized individual, civil, political, and worker rights, as set forth in the Universal Declaration of Human Rights and other international documents. The reports can include specific information on foreign government	
	agencies.	
Non-U.S. Government Tools, Reports, Initiatives, and Guidance <sup>1</sup>		
Freedom in the World Report	Updated each year, this Freedom House report assesses the condition of political rights and civil liberties around the world. The report includes numerical ratings and descriptive text for 195 countries and 14 territories.	
Freedom on the Net Report	Updated each year, this Freedom House report includes ranked, country-by-country assessment of online freedom, a global overview of latest developments, and in-depth country reports. The report includes a color-coded map of countries reviewed showing whether they rank as free, partly free, or not free.	
The Citizen Lab	The Citizen Lab's website includes research on investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.	
Civicus	Maintains an interactive world map providing access to up-to-date information on civic space trends. Website also includes more indepth reporting.	
Global Network Initiative and Country Legal Framework Resource	The Global Network Initiative Principles on Freedom of Expression and Privacy, together with its related Implementation Guidelines, provide guidance to the internet and communications technology industry and its stakeholders in protecting and advancing the enjoyment of human rights globally. The Country Legal Framework Resource explores the legal environment affecting freedom of expression and privacy around the world.	
World Justice Project Rule of Law Index Human Rights Watch Country Reports	Measures how the rule of law is experienced and perceived by the general public in 126 countries and jurisdictions worldwide.  Reports and investigations on human rights abuses around the world.	
Committee to Protect Journalists	Country reports document attacks on the press and obstructions to free press.	

<sup>&</sup>lt;sup>1</sup> This list of tools and guidance is a resource for consideration by exporters. It should not be taken as comprehensive, and does not signify an endorsement of these tools and guidance by the U.S. Government.

Ranking Digital Rights Corporate Indicators	The indicators provide guidance to providers of digital platforms, services and devices on public reporting regarding on human rights, especially privacy and freedom of expression.
	ternational Treaties, Principles, and Guidance
International Covenant on Civil and Political Rights (ICCPR)	The ICCPR is an international human rights treaty adopted by the United Nations in 1966. The U.S. government ratified the treaty in 1992, obligating the U.S. government to protect and preserve human rights identified in the treaty, including the right to be free from arbitrary or unlawful interference with privacy and the right to
	freedom of expression.
UN Guiding Principles on Business and Human Rights	Endorsed by consensus by the UN Human Rights Council in 2011, the Guiding Principles are a set of global guidelines for states and business to prevent, address, and remedy human rights impacts, which involve business enterprises.
The OECD Guidelines for Multinational Enterprises	The OECD Guidelines for Multinational Enterprises are recommendations addressed by governments to multinational
	enterprises operating in or from adhering countries. They provide non-binding principles and standards for responsible business conduct in a global context consistent with applicable laws and internationally recognized standards. The Guidelines are the only multilaterally agreed and comprehensive code of responsible business conduct that governments have committed to promoting. The OECD Guidelines draw upon and are aligned with the UN Guiding Principles on Business and Human Rights. The U.S. government National Contact Point offers a dispute resolution and mediation mechanism when issues arise related to the OECD Guidelines.
OECD Due Diligence Guidance on Responsible Business Conduct	Building on the Guidelines, in May 2018, the OECD released new Due Diligence Guidance for Responsible Business Conduct ("Guidance"). The Guidance elaborates on the due diligence responsibilities of businesses under the OECD Guidelines. It is
	intended to be used in all sectors of the economy and by all companies, regardless of size, geographical location, or value chain position. Its main objective is to help companies understand and implement due diligence responsibilities. The Guidance explicitly refers to risks and impacts, highlighting the need for companies to identify and address these risks and impacts and providing recommendations on how they can do this.

# Appendix 2 – Government Laws, Regulations, and Practices That Could Raise Concerns

The below list is illustrative of the kinds of laws, regulations, and government practices that place the item at a higher risk of misuse. The form of misuse will vary based on the kind of item deployed by the government. Examples of risks include: arbitrarily or unlawfully tracking movements, behaviors, and relationships among vulnerable groups, minority groups, activists, and journalists.

Concern	Example of Laws, Regulations, and Government Practices
Privacy	Allows governments to access domestic computer data and networks, copy information, and/or seize computers or any devices without appropriate safeguards (e.g., subject to review by a transparent and independent judiciary) against unreasonable or abusive government searches and seizures.
	Implements domestically city or nation-wide surveillance or data collection technologies without appropriate safeguards (e.g., subject to review by a transparent and independent judiciary) against unreasonable or abusive government searches and seizures.
	Allows governments to arbitrarily or unlawfully intercept and collect personal information of platform users on broad grounds such as terrorism and "extremism".
	Requires all cyber/internet cafes to install software that tracks and stores information about their clients' online activities.
	Prohibits anonymous profiles on online messenger applications, social media accounts, and other technology driven platforms.
	Implements national or regional facial recognition programs to target or intimidate individuals because they are activists, journalists, or members of vulnerable groups.
	Requires Internet users to install software that enables government officials to monitor communications of all Internet users sent and block individual webpages.
Freedom of Expression	Criminal punishment for speech online (e.g., mobile apps) on the basis that it is blasphemy/apostasy, political/anti-government, disinformation, defamation, anti-national, or toxic content.
	Review and blocking of content published online found objectionable for political reasons, without effective means to request review.
	No or severely restricted independent press, including targeting, harassment, threats, or physical attacks of journalists for their work.
Restricting Civic Space/Targeting	Unduly burdensome procedures or requirements for NGOs to register with the government.
Individuals or Members of Groups on the Basis	Requires NGOs to notify local and national governments about all activities, and gain permission to travel between cities or host fundraisers and protests.
of their Race, Sex, Language, Religion, Political Opinion,	Imposes restrictions, limits, or bans on foreign funding of NGOs.  Requires all domestic and international donor funding to NGOs to be funneled through a government office before reaching the NGO recipient.
National Origin, or any other grounds	Uses spyware to monitor websites, apps, and other digital platforms that cater to a specific minority to target dissidents.
	Prosecutes civil society activists and journalists for exercising their human rights and for advocating on certain issues, under the guise of
	counterterrorism, national security, national identity, or morality.

**DRAFT** 

Total or Significant	Requires companies to provide access to customers' data and Internet
Control over Internet	activities without appropriate safeguards against unreasonable or abusive
Service Providers or	government searches and seizures.
Telecommunications	Requires data to be stored on servers within the country without appropriate
Networks	safeguards against unreasonable or abusive government searches and
	seizures.
	Requires all telecommunications operators to install surveillance equipment
	or comply with laws that allow governments access to all transmitted
	information and other related data, without judicial or other oversight.
	Requires provider to modify service or product to facilitate government
	access to data without appropriate safeguards against unreasonable or
	abusive government searches and seizures.

