October 4, 2019

Mr. Robert A. Destro
Assistant Secretary
Bureau of Democracy, Human Rights and Labor
United States Department of State
Washington, DC 20520

Dear Mr. Destro:

The following comments are submitted by the National Foreign Trade Council (NFTC), the Semiconductor Industry Association (SIA) and the Information Technology Industry Council (ITI) regarding the U. S. Department of State's Draft Guidance regarding the Export of Hardware, Software and Technology with Surveillance Capabilities and/or Parts/Know-How.

Our collective memberships represent companies from the manufacturing, technology, energy, capital goods, transportation, consumer goods, healthcare products, services, e-commerce and retailing sectors. We appreciate the opportunity to offer comments in response to your draft guidance. Our members are committed to respecting international human rights as outlined in the relevant UN treaties. We support government recommendations which align with the UN Guiding Principles on Business and Human Rights (UNGPs) and are pleased to provide our recommendations to refine the non-binding Draft Guidance in line with the expectations of the UNGPs.

I. General

The UNGPs are a process document, outlining broad and high-level due diligence steps companies should take to surface and mitigate human rights risks. The Draft Guidance exceeds the scope of the UNGPs in a number of ways, and should be aligned with the UNGPs through expert and industry input.

In contrast to the Draft Guidance, the UNGPs are *not* prescriptive in what steps can or should be taken, recognizing that one-size does not fit all when it comes to due diligence expectations.The Draft Guidance is also inconsistent with the UNGPs in terms of assessing and addressing risks. The UNGPs recommend prioritizing engagement based on risk, rather than the type of entity or relationship with a government. But the Draft Guidance looks at the type of relationship the end user has with the government of concern and focuses on the "level of control" the latter has over the former, concluding that "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" (*emphasis added*).

To the extent the Guidance is focused on export controls compliance, our member companies are already implementing strong, risk-based compliance programs based on the existing robust legal and regulatory framework for export controls and sanctions. This is important as the Guidance goes well beyond that framework in a number of places. In other places, the Guidance introduces ambiguity with respect to particular terms defined by existing export control regulations (e.g., the EAR definition of cryptanalysis and surreptitious listening devices provide a more nuanced approach than "crypto-analysis products" in the Guidance which could include certain low-end products, such as password guessers and rainbow-table attack tools.)

Recommendation: Reiterate that the expectation for companies is to align with the broad principles outlined in the UNGPs, and revise the Draft Guidance to give businesses more flexibility in designing the appropriate due diligence system for their business and products. At a minimum, the Draft Guidance should clarify that the prescriptive content contained therein serves only as suggestions or a set of examples, and may not be relevant for all companies or all technologies. In addition, the Draft Guidance should clarify and emphasize that an assessment of risks should focus only on severity, rather than on factors that are difficult or even impossible for the private sector to reasonably determine (e.g., level of control a government has over a private entity).

Understanding of Technology and How it is Disseminated

Many definitions in the Draft Guidance are overly broad and lack sufficient clarity. For example, "Items with Intended or Unintended Surveillance Capabilities" is so broad as to capture any ICT product or technology that touches data relayed over communications networks. Estimates show that by 2020 there may be as many as 50 billion digital devices connected to the internet.[1] Surely, the Draft Guidance is not intended to apply to all ICT products that process, relay, or store data over networks.

We have a number of additional questions regarding the broad expectations imposed on busiensses from the draft guidance's ambiguous definitions.

- First, what is the definition of human rights that exporters are to observe? The draft text Appendices 1 and 2 illustrate the impossible task the draft guidance purports to set for businesses– as opposed to the well-defined rationales for precise controls under OFAC and BIS regimes.
- Additionally, the recommendations to "minimize the likelihood" that a product would "be misused to commit human rights violations or abuses" are not practical and, in some cases, contrary to international cybersecurity norms and best practices. For example, the admonition to build a "kill switch" into a product or "limit upgrades, software updates, and direct support" could create significant vulnerabilities in the device and/or network that may enable network exploitation or otherwise damage network security. Further, building a "kill switch" into a product could in fact enable bad actors to infringe on the human rights of citizens in other ways, for instance to enable internet censorship and stymie freedom of expression (such as happened in the Arab Spring). The interagency capacity of the U.S. government – as manifest in Commerce, Treasury, and State control regimes – to identify

[1] https://medium.com/datadriveninvestor/50-billion-connected-devices-by-2020-b55e0656f5c9.

and proscribe human rights violators in concert with other considerations germane to national security speaks for itself. Private sector companies are not equipped nor mandated to do so in any sustainable way.

- Further, nowhere in the UNGPs does it talk about responsibility for "unintended" consequences from products. Instead, the UNGPs talk about actual and potential human rights abuses that businesses can cause or contribute. This is a critical difference and a determinant of ultimate responsibility.

We also point out that the due diligence provisions in the Draft Guidance do not distinguish between off-the-shelf products that are mass marketed through multiple distribution channels and customized products that are built for specific needs of known customers. This lack of distinction creates a number of technical and economic challenges, e.g., applying "integration of safety and 'privacy by design' features" the same way to mass marketed and customized products.

Recommendation: The Draft Guidance should provide a narrow definition of the type of items in scope, focusing on "categories of items that impact surveillance" " – with a focus on end equipment rather than individual components – and providing more specific examples of technology that directly cause or contribute to the harm. The Draft Guidance also should make it clear that customized products that fall within its scope can pose higher risks, but also more opportunities for application of the suggested risk mitigation measures.

II. Scope of Due Diligence

The UNGPs outline the need to conduct human rights due diligence on "human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationship." Importantly, the UNGPs outline that a company should assess risks at a *broad* level, and then design additional due diligence efforts where impacts are most salient. The UNGPs are not prescriptive about what those additional efforts should be.

In contrast and contrary to the UNGPs, the USG Draft Guidance is extremely detailed and appears to apply the same way to all companies, all technology products – end equipment and components alike – and all risks.

Recommendation: Consistent with UNGPs, the Draft Guidance should recommend a high-level human rights impact assessment as a first step that, in alignment with the UNGPs and include as assessment of third parties. Additional due diligence activities should be dependent on the findings of the initial assessment. This more flexible framework would be able to take into account natural and significant variations in product capabilities, risks, and misuses.

III. Product Development Guidance

The UNGPs highlight that "in order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes *appropriate to their size and circumstances*" (emphasis added).

As noted earlier, the Draft Guidance asks companies to "integrate safety and 'privacy by design' features" to minimize the likelihood of misuse, and includes examples of the types of features companies may employ.

Recommendation: Consistent with the UNGPs and our earlier recommendations, the Draft Guidance should allow much more flexibility in its due diligence framework and make it clear that any process expectations are not a one-size-fits-all.

IV. Due Diligence on End Users

The UNGPs recognize the importance of assessing risks related to business partners. "Know Your Customer" due diligence has been found to be an effective tool in assessing potential risks related to technology sales.

However, due to the complex and varied nature of some distribution channels in the technology industry, with mass marketed products it often is difficult (if not impossible) to understand the ultimate uses of all end users and sufficiently perform the diligence described in the Draft Guidance. In addition, while the red flag that is focused on a government end-user that "has a history of exporting items to other countries with authoritarian governments and history of committing human rights violations or abuses" is clear, the red flag that takes into account "'ongoing conflict' or 'political turmoil' in region being exported to," is far too broad as the terms used are general and vague.

Recommendation: Provide illustrative guidance for how companies could address sales in cases where the ultimate end use may not be known, but the product in question could cause a serious impact if misused. For example, companies could consider requiring end use agreements where effective or require partners to conduct their own human rights due diligence in cases of resale.

V. Grievance Mechanism

The UNGPs outline that "where business enterprises identify that they have *caused* or *contributed* to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes" (emphasis added).

The USG Draft Guidance includes language regarding the development and use of grievance mechanisms, but does not specify when a company would be responsible for the provision of a remedy. This creates uncertainty and potentially a massive burden to industry if such mechanisms are overapplied. For example, as drafted, the guidance could be interpreted to suggest that the grievance mechanisms should apply to an individual component or input that, by itself, does not cause or contribute to an adverse impact to human rights but is included in a product or system that does. In addition, the Draft Guidance suggests a number of prescriptive "contractual safeguards" without acknowledging that some of them may not be effective or acceptable to customers (e.g., the right to "unilaterally terminate the contract … in its sole discretion" is unacceptable to many customers that need a stable and secure supply chain).

Moreover, we note that requiring manufacturers to reassess a technology product after it has been shipped and used can be extremely difficult—especially for mass marketed products. In addition, it is not appropriate, or realistic, to request that any and all suppliers of technology products or components always "remotely disable the item, and limit upgrades and customer support when a credible complaint of misuse is received, until the investigation is complete." Although a complaint may be credible, it could be causing a minor incident (or none at all) yet cutting off technology support could cause other human rights abuses and/or major economic consequences to a customer's multiple end users (e.g., if the product processes major streams of commercial data). As noted earlier, a number of provisions in the Draft Guidance do not seem to take into account how technology works in the real world.

Recommendation: Revise the Grievance Mechanism section to reference the effectiveness criteria outlined in Principle 31 of the UNGP and clarify that companies would only be responsible for providing remedy in cases where the company has caused or contributed to an adverse human rights impact. Specifically acknowledge that in certain cases the suggested contractual safeguards may not be commercially feasible, and the other suggested mitigation measures may not be technically feasible or otherwise appropriate.

VI. Reporting

The UNGPs ask that companies communicate externally on their human rights due diligence activities while ensuring that reporting does "not pose risks to affected stakeholders, personnel or to legitimate requirements of commercial confidentiality."

The USG Draft Guidance asks companies to publicly report on the export transaction. This creates multiple risks, including possible breaches of confidentiality that are an exception to the reporting per the UNGPs.

Recommendation: Limit the reporting recommendation to *process steps* during the product development phase, rather than a reporting on individual incidents (unless they are severe and there are no safety or other risks to the stakeholders involved). Include a recognition that public reporting may present risks to the company and rightsholders and that reporting should be focused to limit these risks. Acknowledge, as noted by the UNGPs, that such reporting may vary according to the enterprise and its circumstances.

VII. Commercial Challenges

The UNGPs outline that the "responsibility of business enterprises to respect human rights applies to all enterprises regardless of their size, sector, operational context, ownership and structure. Nevertheless, the scale and complexity of the means through which enterprises meet that responsibility may vary according to these factors and with the severity of the enterprise's adverse human rights impacts."

The Draft Guidance includes some risk mitigation recommendations that likely would be very arduous and significantly impact business functions and even a company's viability. Specifically, in its instructions the Draft Guidance does not account for the significant commercial

considerations of the different manufacturing and market circumstances exporters routinely face. For example, depending on the product at issue, at least some of the technical mitigations listed in the guidance may not be technically feasible (e.g., kill switch and auto delete data functions). But even if they are technically feasible, some of those features could be commercially impractical for many companies (e.g., costs more money than companies would make on product, and not be commercially appealing resulting in a loss of customers). In other words, in addition to practical challenges for many exporters of mass marketed products (e.g., the requirement to "alert the exporter to misuse"), there may also be serious commercial challenges (e.g., many customers would balk at the requirement that a manufacturer have ability to "limit the use [of the product] once sold"). These commercial challenges must be taken into account because of the ultra-competitive environment technology companies live in where profit margins often are very small, and some foreign technology companies will use every advantage they have to get customers to "design out" U.S. technology.

Recommendation: Reference the guidance from the UNGPs that the "scale and complexity of the means through which enterprises meet that responsibility may vary according to these factors and with the severity of the enterprise's adverse human rights impacts." Make it clear that its safety and privacy by design features are merely individual suggestions, not additive, and that they may not be technically and/or commercially feasible in many cases.

VIII. Human Rights Tools and Guidance

In addition to the resources provided, we would recommend adding the UN Universal Periodic Reviews (UPR) available at: https://www.ohchr.org/en/hrbodies/upr/pages/uprmain.aspx. The UPR involves a review of the human rights records of all UN Member States. The UPR is a State-driven process, under the auspices of the Human Rights Council, which provides the opportunity for each State to declare what actions they have taken to improve the human rights situations in their countries and to fulfil their human rights obligations.

IX. Conclusion

Thank you for the opportunity to provide comments. We appreciate your commitment to these critical issues and your consideration of the points raised.

Sincerely,

Information Technology Industry Council (ITI)
National Foreign Trade Council (NFTC)
Semiconductor Industry Association (SIA)