Before the
U.S. Department of Commerce
Washington, D.C.

In re:
Proposed Rule: Securing the Information and Communications Technology and Services Supply Chain

Docket No. 191119-0084
84 FR 65316

COMMENTS OF
INTERNET ASSOCIATION

Internet Association (IA) welcomes the opportunity to engage on the Department of Commerce's proposed rule regarding Executive Order 13873, Securing the Information and Communications Technology and Services (ICTS) Supply Chain. The proposed rule provides the U.S. government with the authority to intervene in, and potentially block, commercial transactions on national security grounds. IA appreciates that Commerce issued this as a proposed rule with an opportunity for public comment given the significance of this rule to U.S. companies.

As currently drafted this proposed rule is overly broad and would adversely impact America's digital economy. Accordingly, IA urges the Department of Commerce to revise the proposed rule with a focus on identifying concrete risks and narrowly defining terms to address those risks. The industry is committed to working with the Department of Commerce on ways to ensure national security objectives are met without unnecessarily undermining U.S. companies' competitiveness.

IA represents over 40 of the world's leading internet companies.[1] IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA supports policies that promote and enable internet innovation, ensuring that information flows freely and safely across national borders, uninhibited by restrictions that are fundamentally inconsistent with the open and decentralized nature of the internet.

American-based internet companies are a significant driver of the U.S. economy and U.S. exports. The internet sector is now the fourth largest sector in the U.S. economy, contributing $2.1 trillion to the U.S. economy in 2018, accounting for 6 million direct jobs and another 13.1 million indirect jobs in other areas of the economy, and investing over $60 billion into the economy each year.[2]

Small businesses and entrepreneurs in every state and every community use the internet to sell and export across the globe. Digital trade now accounts for more than 50 percent of all U.S. services exports. Internet-connected small businesses are three times as likely to export and create jobs, grow four times more quickly, and earn twice as much revenue per employee.[3] Digital trade and digital trade-enabled businesses contribute more than $450 billion in exports annually, which helps account for the U.S.'s $178.3 billion trade surplus in digital services.[4]

It is critical the U.S. government avoid promoting policies that adversely impact internet companies and their substantial contributions to the U.S. economy. IA has concerns that, as drafted, the

[1]https://internetassociation.org/our-members/
[2]https://internetassociation.org/publications/measuring-us-internet-sector-2019/
[3]https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-connected-small-businesses-Jan2018.pdf
[4]https://internetassociation.org/files/ia_securing-americas-digital-trade-leadership/

proposed rule lacks important procedural and substantive safeguards that are essential to a fair, transparent, and effective regulatory regime. As a result, it could create significant adverse consequences for U.S. businesses and U.S. digital leadership without a corresponding benefit to U.S. national security.

The rule should be narrowed to address identifiable threats. The internet industry believes that the proposed rule's broad scope and unprecedented grant of discretion risks unintended harm to U.S. digital leadership. While there are legitimate concerns about certain foreign-sourced technologies, IA worries that, unless the approach is appropriately calibrated, the proposed rule could do lasting harm to U.S. global digital leadership. The broad scope of transactions potentially subject to review and the nearly unlimited discretion granted to the Secretary mean that virtually all international interactions of U.S. digital companies could require regulatory review. Any business partners outside the U.S. may then hesitate to enter into relationships with U.S. companies, for fear that those relationships could be suddenly and unexpectedly severed, which would effectively isolate the U.S. digital sector from the rest of the world.

Greater certainty in the application of the proposed rule would be beneficial for all interested parties. As drafted, the rule potentially covers millions of ICTS transactions, regardless of their level of risk and whether they are already covered by existing regimes, such as ECRA/EAR, Team Telecom, and FIRRMA/CFIUS. This rule must be narrowed to define specific ICTS of concern, or to categorically exclude a large number of ICTS that are low-risk, or can be effectively mitigated through compliance programs. A non-exhaustive list of examples of exclusions includes: (1) mass market electronic devices primarily intended for home or small office use; (2) commercial off-the-shelf (COTS) items that do not require modification or maintenance over their lifecycle; (3) software designed for commercial use; and (3) outbound transactions covered by existing regimes, such as EAR and ITAR.

Key terms should be defined or clarified. The scope of the proposed rule requires further calibration and clarity. In its current form, the scope of transactions that may be subject to review under the proposed rule is incredibly broad and vague, making it nearly impossible for U.S. companies to plan, and putting U.S. internet leadership at risk.

Although the preamble describes a "case-by-case, fact-specific approach intended to avoid overly restricting entire classes of transactions," Executive Order 13873 and the proposed rule fail to provide for a process that will give meaningful notice to potentially impacted parties. The result is that companies must operate in an environment where all ICTS transactions are within scope.

Commerce must be more specific about who "foreign adversaries" are, and tie this determination to clear criteria. When making the determination, it is important that whole countries not be deemed to be "foreign adversaries." This is critical to ensure certainty for businesses entering into ICTS transactions.

The definition of terms in the proposed rule also raise concerns. For example, the term "transaction" should be revised to remove "dealing in" and "use of." This characterization is too broad and there is no way to know in all cases whether stakeholders will be captured merely for using or "dealing in" an item. Similarly, the inclusion of transactions that pose an undue risk to the "digital economy" could potentially mean any transaction. This should be removed to focus instead on concrete national security concerns.

The criteria for reviewing a transaction should be narrowed and transparent. The criteria for reviewing an ICTS transaction are also vague and should be revised to narrow potential applications. For example, the phrase "subject to the jurisdiction of the United States" is overly broad and potentially captures the activities of U.S. foreign subsidiaries that occur outside of the United States. Similarly, the Department of Commerce should strike the reference to persons "subject to the jurisdiction or direction of" a foreign adversary. This definition could apply to any person - regardless of their citizenship -

located in a foreign country where the government is deemed a foreign adversary. The interest of a "foreign country or a national thereof" is not relevant to the evaluation because transactions should only be evaluated when they are tied to an identifiable foreign adversary.

Commerce should also be willing to provide advisory opinions when requested to provide further clarity. Relatedly,there should be a process for companies to submit a notification of a transaction, and receive safe harbor protection if Commerce declines to undertake an inquiry after a reasonable time frame).

Mitigation should always be the goal. The Department of Commerce should look to mitigation in all cases, prohibiting or unwinding transactions only as an option of last resort. As drafted, the proposed rule provides equal weight to transaction prohibition and mitigation outcomes following a review. This balance should be weighted heavily toward mitigation outcomes, limiting the prohibition or unwinding of transactions to those situations in which mitigation would be impossible, or incredibly impractical.

A formal interagency process should be established. The broad authority granted to the Department of Commerce requires clear interagency accountability measures. The proposed rule also gives the Secretary of Commerce an extraordinary amount of discretion, which creates a lack of transparency that makes it extremely difficult for U.S. companies to accurately assess and comply with regulatory obligations and/or restrictions. Commerce should consider establishing a more formalized interagency vetting process across the national security agency reviewers with clearly defined review criteria.

IA believes that a process where impacted agency heads are required to convene for a session or conduct a vote on whether a transaction is subject to the proposed rule, whether it poses a risk to national security, and the appropriate enforcement measures, would ensure that all interested agencies are afforded the opportunity to provide input on key decisions that will impact the critical infrastructure of the United States. In developing a new structure, the formal rules surrounding CFIUS could act as a guide.

Determinations should be transparent, yet protect confidentiality. Additionally, the Department should be required to publish a public report in the Federal Register annually on the number of transactions reviewed, blocked, and mitigated, but without disclosing the names of the parties involved. The report should also describe, on an unclassified basis, and without revealing party names, the category of ICTS involved and the national security rationale for the Department's actions in each case in order to provide notice to those in the ICTS community on areas of enforcement. The Department should provide a more detailed report to Congress.

Creating further uncertainty for U.S. companies, the proposed rule allows the Secretary to dispense with the limited processes established under the rule by declaring an "emergency." The criteria for dispensing with the procedures are extremely broad: "when public harm is likely to occur … or national security interests require it." The Secretary – or his or her "designee" – has virtually no accountability for such a sweeping exercise of authority, beyond simply including "the basis for the decision" in a final written determination. As drafted, this portion of the proposed rule would allow an unelected, unconfirmed, and ultimately unaccountable official to order momentous changes to the commercial activities of American companies. Regardless of whether the criteria for declaring an emergency are amended, Commerce should adopt an appeals process for those notified of a decision under the emergency authority in order to provide them the opportunity to respond and mitigate the impact of the declaration.

The proposed rule raises a number of additional process-oriented concerns that compound its vague and ambiguous terms. In drafting a more targeted, clear rule, the Department of Commerce should include language to specifically address the following concerns:

- Private party information submissions present risks for abuse. Commerce should not use private party submissions as a basis for reviewing transactions unless they can be corroborated.
- Any review undertaken by Commerce should be subject to strict deadlines so that businesses can make informed decisions.
- Commerce should only look at pending or future transactions. Looking backward and calling for a transaction to be unwound years after the fact is untenable.
- There should be a mechanism created to appeal potentially problematic determinations.

Conclusion.

In conclusion, as drafted, the proposed rule lacks important procedural and substantive safeguards that are essential to a fair, transparent, and effective regulatory regime. This proposed rule could create significant adverse consequences for U.S. internet businesses without a corresponding benefit to U.S. national security. The internet industry strongly urges the Department of Commerce to reconsider the approach this rule takes, taking into account the comments above. IA looks forward to working with the administration on a way forward.