



Questions for the Record

Import Controls: Tools to Counter the CCP's Industrial Policy and Supply Chain Threats

9/16/2026

Representative Zach Nunn – District 3

Witness – Mr. Peter Harrell

1. You've advocated for the U.S. to develop a clear, systematic framework for national security import controls, rather than responding to threats on an ad hoc basis. I saw the importance of getting ahead of these threats during my time at the National Security Council, when Huawei was raising serious concerns about the security of our networks. Today, that challenge goes well beyond telecommunications. China is looking for vulnerabilities across our economy, from connected vehicles to the inputs our farmers rely on.

From an operational standpoint, how should we be prioritizing which industries—like agriculture or connected vehicles—get targeted for national security import controls first?



Answer: Thank you for the question. As I noted in my written statement, I recommend that the U.S. established structured, proactive process to identify products where imports potentially pose national security risks. The process that the Commerce Department's Office of Information and Communications Technology Security (OICTS) established in 2023 and 2024, in which it convened interagency partners to solicit input for a structured list of ICTS products to focus on, provides a potential model, though that process focused only on internet connected equipment, not the broader range of imported products that potentially pose national security risks. In my view either the Commerce Department or the Pentagon could lead such a process, in consultation with other agencies.

The review process should evaluate candidate products against at least four criteria:

- How severe is the potential harm? For example, products that could cause widespread disruptions to critical infrastructure, or facilitate espionage, can create particularly severe harms.
- Can an adversary have ongoing control of a product? (Products that connect to the internet and receive remote software updates can pose long-term risks because an adversary can exploit them long after they are sold).
- How concentrated is our dependence? Where China supplies a large share of a product, or controls a chokepoint component, Beijing has leverage it could use in a crisis.
- Do trusted alternatives exist, or can we build them?

I recommend that whichever agency is responsible for leading this process publish an annual list of priority products that would both show the American people and corporate sector what the government priorities are and help drive government focus.



2. Are there specific metrics or thresholds that should trigger a mandatory mitigation response, so these agency risk assessments lead to real enforcement instead of sitting on a shelf?

Answer: I think specific metrics or thresholds could potentially be set to force an investigation into whether the government should restrict imports of a product, but that any decision on actual restrictions should be left to the government's discretion, given that import bans can create complex unintended consequences. A rigid trigger that mandates a specific ban, for example, could cut off a product before the U.S. is able to develop trusted, non-Chinese alternatives.

Metrics or thresholds themselves, however, also need to be tailored to the type of product, rather than adopting a one-size-fits-all model. For example, for a product such as a specialty industrial chemical, a 50% or more dependency on China as a supplier should potentially trigger a review to determine if dependence on China provides China with a geopolitical leverage. But for products such as communications equipment, that pose ongoing risks, a much lower dependency threshold would probably be appropriate to trigger an investigation.

Two additional steps are important to make the system work. First, any decision to restrict a product where U.S. or allied alternatives are limited should come with a plan to start producing them, so that a mandatory response does not simply leave Americans without access to valuable technologies. Second, agencies should periodically report whether existing controls are actually reducing the risk they were meant to address and evaluate the effectiveness of the controls.