


# Shining Some Light on CFIUS's Black Box: Biden Administration Releases An Updated List of High-Priority Critical and Emerging Technologies

In October 2020, the White House published the [National Strategy for Critical and Emerging Technologies](#) ("NSCET"). The NSCET identifies 20 high-priority technology areas that are regarded as critical, or potentially critical, to the United States' national security advantage, including military, intelligence, and economic advantages. According to the NSCET, the U.S. Government's strategy is to continue to maintain technology leadership in each of these high-priority areas, and to remain vigilant in protecting the United States' technology advantage from a variety of licit and illicit technology transfer mechanisms.

In February 2022, a subcommittee of the National Science and Technology Council ("NSTC") published a new report titled, "[Critical and Emerging Technologies List Update](#)" (hereinafter, "NSTC Report"). The NSTC Report updates the NSCET's initial list of high-priority technology areas by reducing the number of technology areas, changing the names of some of the technology areas, and including "subfields" for each of the technology areas. The subfields provide more particularized examples of technologies that are regarded as a high priority by U.S. Government agencies.

The NSTC Report notes that the updated list of critical and emerging technologies (hereinafter, "Updated CET List") should be used as a resource to: "inform future efforts that promote U.S. technological leadership; cooperate with allies and partners to advance and maintain shared technological advantages; develop, design, govern, and use CETs that yield tangible benefits for society and are aligned with democratic values; and develop U.S. Government



measures that respond to threats against U.S. security.” The NSTC Report also notes that “[d]epartments and agencies may consult this CET list when developing, for example, initiatives to research and develop technologies that support national security missions, compete for international talent, and protect sensitive technology from misappropriation and misuse.”

To be clear, the Updated CET List was not published directly by CFIUS, but rather by a subcommittee of the NSTC. However, a majority of the CFIUS member agencies, including the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the Department of State, the Department of Commerce, and the Office of Science and Technology Policy, were members of the NSTC subcommittee and participated in the interagency review process that led to the publication of the NSTC Report and the Updated CET List. In fact, it is likely that at least some of the government offices that served on the interagency committee that published the NSTC Report are the same offices that have a seat at the table during CFIUS’s weekly interagency meetings. Accordingly, the NSTC Report gives dealmakers some insight into the types of critical and emerging technologies that CFIUS is focused on safeguarding from licit and illicit technology transfer mechanisms. Indeed, as noted above, the NSTC Report expressly states that agencies may use the Updated CET List as a tool to “protect sensitive technology from misappropriation and misuse,” which suggests that CFIUS member agencies may use the Updated CET List a resource when evaluating CFIUS filings.

Put differently, CFIUS’s regulations do not provide a unique definition of “critical technology.” Instead, the regulations define “critical technology” primarily as any item that appears on certain export control lists. But anyone familiar with CFIUS knows that CFIUS’s focus is broader than the export control lists. Because CFIUS does not publish any comparable list of critical and emerging technologies or provide any specific guidance on technologies of concern, the Updated CET List is one of the only publicly available windows into CFIUS’s thinking about critical technologies. To be sure, the Updated CET List, like the initial critical and emerging technologies list, remains a relatively vague document; the subfields themselves are broad categories of technologies. But if dealmakers want a concise list of technologies that CFIUS member agencies are concerned about protecting, the Updated CET List is a

---

good resource.

Any dealmaker involved in a transaction where the target U.S. business is providing products or services involving any of the technology areas or subfields in the Updated CET List should strongly consider submitting a CFIUS filing. Even if the filing is not mandatory, a transaction involving critical and emerging technologies is exactly the type of transaction for which CFIUS's non-notified team is most likely to require a post-closing filing. The Updated CET List is not, and does not purport to be, a comprehensive list of all the advanced technologies that CFIUS might be focused on protecting, and the fact that a transaction does not involve any of the technology areas on the Updated CET List does not necessarily mean that CFIUS will not be concerned about the transaction. Moreover, the Updated CET List does not directly touch upon critical infrastructure or sensitive personal data, which are high-priority areas for CFIUS. But the fact that a transaction involves one of the technologies on the Updated CET List is, at a minimum, an early warning sign that a transaction may have CFIUS risk.

Click [here](#) to view the Updated CET List with subfields.

---

## Authors



Tyler McGaughey

Partner, Yuanda

Washington, D.C.

+1 202-282-5306

[tmcgaughey@winston.com](mailto:tmcgaughey@winston.com)