Proskauer

White House Updates Critical and Emerging Technologies List to Address AI, Data Security, Space and Geopolitical Competition

Regulatory & Compliance on **March 1, 2024**

Implications for CFIUS Reporting and Review

The Executive Branch, through the National Science and Technology Council and the National Security Council, committed in 2020 to identify that are potentially significant to U.S. national security. The 2024 update was released on February 12, 2024. Updated every two years, the CET list is the product of extensive interagency deliberations, and " …builds upon earlier lists and may inform government-wide and agency-specific efforts supporting U.S. technological competitiveness and national security."

The February 2024 CET list update identifies the following subfields:

- Advanced Computing
- Advanced Engineering Materials
- Advanced Gas Turbine Engine Technologies
- Advanced and Networked Sensing and Signature Management
- Advanced Manufacturing
- Artificial Intelligence
- Biotechnologies
- Clean Energy Generation and Storage
- Data Privacy, Data Security, and Cybersecurity Technologies
- Directed Energy
- Highly Automated, Autonomous, and Uncrewed Systems (UxS), and Robotics
- Human-Machine Interfaces
- Hypersonics
- Integrated Communication and Networking Technologies

- Positioning, Navigation, and Timing (PNT) Technologies
- Quantum Information and Enabling Technologies
- Semiconductors and Microelectronics
- Space Technologies and Systems

The 2024 CET list update places greater priority than prior iterations on data security, artificial intelligence, space and geopolitical competition, among other areas.

The Executive Branch updated the CET list to reflect the complexities surrounding recent artificial intelligence developments. The Artificial Intelligence subfield now includes foundational models, generative AI systems, multimodal, and large language models, as well as technologies for improving AI safety, trust, security, and responsible use.

Further highlighting the practical implications of automation, the former Autonomous Systems and Robotics subfield has been enhanced to include supporting digital infrastructure, including High Definition (HD) maps.

The Semiconductors and Microelectronics subfield, revised from the 2022 update, maintains a prominent role in the list, re-emphasizing specialized/tailored hardware components for artificial intelligence, natural and hostile radiation environments, RF and optical components, high-power devices, and other critical applications. It newly includes novel architectures for non-Von Neumann computing.

The 2022 update identified the Financial Technologies subfield, which has now been replaced with the Data Privacy, Data Security, and Cybersecurity Technologies subfield. The new subfield includes privacy-enhancing technologies, computing supply chain security, and security and privacy technologies in augmented reality/virtual reality.

Following the themes of privacy and cybersecurity, the updated Integrated Communication and Networking Technologies subfield adds delay-tolerant networking, modern data exchange techniques, and resilient and adaptive waveforms. Additionally, Positioning, Navigation, and Timing (PNT) Technologies is its own subfield in this update. The PNT subfield adds interference, jamming, and spoofing detection technologies, algorithms, analytics, and networked monitoring systems. Disruption/denial-resisting and hardening technologies are also featured in the new PNT subfield.

The Space Technologies subfield is significantly enhanced, in line with today's geopolitical competition. The subfield now includes resilient and path-diverse space communication systems, networks, and ground stations. It also adds technologies that enable access to and use of cislunar space and/or novel orbits, and elaborates on sensors and data analysis tools for space-based observations.

The 2024 CET list update reflects the Executive Branch's technological priorities to strengthen national security, should be considered in step with other national security efforts by the administration and has implications for CFIUS coverage, reporting, filings and reviews as the Committee takes the new priorities into account.

On February 28, 2024, two weeks after the 2024 update, the Department of Justice announced the President's first of its kind Executive Order (EO) to address the extraordinary national security threat to Americans' bulk sensitive personal data and U.S. government-related data, posed by six countries of concern: China, Russia, Iran, North Korea, Cuba, and Venezuela. Attorney General Merrick B. Garland announced: "This Executive Order gives the Justice Department the authority to block countries that pose a threat to our national security from harvesting Americans' most sensitive personal data—including human genomic data, biometric and personal identifiers, and personal health and financial data."

View Original

Related Professionals

- **John R. Ingrassia**
  Partner