Debevoise National Security Update: Supply Chain Security in 2024

March 11, 2024

Barely two months into the new year, the Biden-Harris Administration has already issued several significant measures in 2024 intended to strengthen the security of American supply chains from national security threats. Congress has also increased scrutiny over supply chain security from countries designated as foreign adversaries and forced labor. These actions are significant because they confirm that the U.S. federal government continues to create regulatory tools to compel companies to monitor their supply chains. Affected parties should monitor these developments and re-tailor their supply chain security programs to their respective risk.

This client alert addresses the implications for affected parties of the U.S. government's most significant supply chain security measures and trends for 2024.

Executive Order to Protect Americans' Sensitive Personal Data

As detailed on the Debevoise & Plimpton Data Blog, on February 28, 2024, President Biden issued *Executive Order 14117 Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*.[1] The order expanded the scope of a previous executive order, Executive Order 13873, which was intended to strengthen efforts to prevent countries designated as foreign adversaries from exploiting vulnerabilities in the information and communications technology and services ("ICTS") supply chain.[2]

Executive Order 14117 establishes a framework for the Department of Justice ("DOJ") and other agencies to prevent the large-scale transfer of Americans' personal data to "countries of concern," which are preliminarily defined as China and Russia, among others. The categories of protected data include genomic data, biometric data, personal

[1] *See Biden Administration Acts to Limit Access to Sensitive Personal Data by Countries of Concern*, debevoisedatablog.com (March 5, 2024), *available at* https://www.debevoisedatablog.com/2024/03/05/biden-administration-acts-to-limit-access-to-sensitive-personal-data-by-countries-of-concern/.

[2] *See* Exec. Order No. 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 F.R. 15421 (2024) (Feb. 28, 2024).

health data, geolocation data, financial data and certain kinds of personally identifiable information. Among other things, the order recognizes that access to such bulk personal data by countries of concern "through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements poses particular and unacceptable risks to our national security."[3] The order therefore expands the role of DOJ to regulate the use of these mechanisms to obtain and exploit American data, including by directing it to issue regulations to protect sensitive U.S. data from exploitation due to large-scale transfer to countries of concern. As a result, DOJ concurrently released an Advanced Notice of Proposed Rulemaking ("ANPRM") detailing potential definitions for key terms not defined in the order.

Accordingly, companies with supply chains that either include or otherwise rely on large-scale transfer of Americans' personal data (including through vendors) should closely monitor DOJ's implementing regulations. Companies should be prepared to adjust segments of their supply chains that implicate risk of such data being transferred to China, Russia or other countries of concern.

Department of Commerce Investigation into Connected Vehicles

The day after Executive Order 14117 was issued, the Department of Commerce ("DOC") announced that it was opening an investigation into the ICTS supply chain for "connected vehicles."[4] Citing its authorities under Executive Order 13873, the DOC issued an ANPRM that signals it is contemplating regulations to address the national security risk from Chinese manufactured technologies used in connected vehicles. The ANPRM seeks input to define the term "connected vehicle," although it provides that the term could constitute an "automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device."[5] While DOC's public messaging regarding the investigation has focused on reducing any national security threat from data collection from Chinese manufactured cars before they are imported into the United States, the ANPRM appears to provide leeway for future

---

3 *Id.* § 1.

4 *See Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles*, commerce.gov (Feb. 29, 2024), *available at* https://www.commerce.gov/news/press-releases/2024/02/citing-national-security-concerns-biden-harris-administration-announces.

5 *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 89 F.R. 15066 (March 1, 2024).

regulations to also address non-Chinese vehicles that contain Chinese software or hardware parts in their supply chains.

While the DOC's investigation into connected vehicles is just beginning, the fact that the Department is exercising its ICTS authority is significant on its own. It signals that the Biden-Harris Administration is prioritizing further regulations and future enforcement actions to secure the ICTS supply chain. Moreover, the Department of Commerce has repeatedly called on Congress to pass the RESTRICT Act, which would codify its ICTS authorities in statute and provide an even stronger foundation for forthcoming regulations and enforcement actions.

Department of Defense List of Chinese Military Companies

Pursuant to Section 1260(H) of the National Defense Authorization Act ("NDAA") of 2021, the Department of Defense ("DOD") maintains a public list of Chinese military companies that operate directly or indirectly in the United States ("1260H List"). The list includes Chinese companies that span a wide range of industries, including telecommunications, aerospace, automotive, electronics, semiconductors, and other ICTS sectors. On January 31, 2024, DOD updated the 1260H list by adding 17 new entities and removing three.[6] Notably, DOD added IDG Capital Partners Co., Ltd., which is the first 1260H designation of a Chinese investment firm, and signals that DOD will list private equity and venture capital firms due to national security concerns that may arise from their investments. Other additions include artificial intelligence company Beijing Mgvii Technology Co. and technology company NetPosa Technologies, Ltd.

Although designations on the 1260H List currently have no legal effect, that will soon change as a result of Section 805 of the 2024 NDAA. That provision provides that, effective June 30, 2026 and subject to certain exceptions, DOD may not enter into, renew, or extend a contract for goods, services or technology with any entity designated on the 1260H List or entities that they control (the specifics of which will be determined by DOD's forthcoming implementing regulations). Effective June 30, 2027, DOD will also be prohibited from purchasing end products or services produced or developed by an entity on the Section 1260H List indirectly through third parties. Congress is also

---

[6] *See DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021*, defense.gov (Jan. 31, 2024), *available at* https://www.defense.gov/News/Releases/Release/Article/3661985/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.

actively considering legislation that would impose sanctions on 1260H entities, thereby signaling that 1260H designation could form the basis for additional punitive measures.[7]

Companies that contract with DOD should continue to monitor the 1260H List. Although the direct effect of 1260H List designations is currently limited, companies with designated entities in their supply chains could still raise security concerns for federal agencies. Companies will plausibly have to rid 1260H List entities from their supply chains should they desire to contract with DOD after June 30, 2027.

Uyghur Forced Labor Prevention Act Enforcement

Companies in Uyghur Forced Labor Prevention Act ("UFLPA") priority sectors should take note of enhanced enforcement and increased congressional scrutiny of supply chains. Since mid-February, reports have surfaced that U.S. Customs and Border Protection ("CBP") impounded thousands of Volkswagen Group's Bentley, Porsche and Audi vehicles under the UFLPA, purportedly following Volkswagen's voluntary disclosure that the vehicles contain a transformer built by an entity on the UFLPA Entity List.[8]

These enforcement actions follow a January 22, 2024 bipartisan letter from Chairman and Ranking Member of the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (the "Committee") to the Department of Homeland Security ("DHS"), urging it to enhance UFLPA enforcement.[9] The Committee identifies several facets of DHS's UFLPA enforcement about which it is "deeply concerned," including in critical minerals, gold, and rare earth minerals found in supply chains of American companies.

To remedy the perceived underenforcement, the Committee urges DHS to, among other things, (1) add companies located outside of Xinjiang and China to the UFLPA Entity List; (2) "urgently expand" collaboration with the DOJ's "Trade Fraud Task Force" ("Task Force"), which prosecutes companies for violating U.S. trade statutes; and (3) to strengthen cooperation with the Task Force and other agencies to "increase criminal

---

7 *See* Chinese Military and Surveillance Company Sanctions Act of 2023, H.R. 760, 118th Congress (2023).

8 *See The Blacklisted Component That's Disrupting the Luxury-Car Market*, wsj.com (March 6, 2024), *available* at https://www.wsj.com/business/autos/the-blacklisted-component-thats-disrupting-the-luxury-car-market-df87a3b3; *US Porsche, Bentley and Audi Imports Held Up Over Banned Chinese Part*, ft.com (Feb. 14, 2024), *available at* https://www.ft.com/content/ab63cc9b-1c57-43d0-89c2-8f63e5c06eba.

9 *See Letter to Secretary Mayorkas on Enforcement of the Uyghur Forced Labor Prevention Act*, selectcommitteeontheccp.house.gov (Jan. 22, 2024), *available at* https://selectcommitteeontheccp.house.gov/media/letters/letter-secretary-mayorkas-enforcement-uyghur-forced-labor-prevention-act.

prosecutions" against entities in UFLPA priority sectors (tomatoes, cotton, and polysilicon-based products), critical minerals, and seafood industries. The letter also provides a list of 29 entities for DHS and the interagency Forced Labor Enforcement Task Force to consider adding to the UFLPA Entity List, which includes fishing companies, seafood suppliers, and companies that mine and process gold and other minerals.

Companies whose products include materials of the kind produced by the 29 entities identified by the Committee should verify whether they are in compliance with UFLPA. In light of expected increases in DHS enforcement following the letter, companies should also continue to ensure that components of their supply chain monitoring programs are tailored to their risk, including by employing mapping, audits, and trainings as necessary.[10]

Department of Homeland Security Maritime Supply Chain Measures

On February 21, 2024, DHS announced several measures to secure the supply chain of American maritime critical infrastructure.[11] Most notably, the U.S. Coast Guard ("USCG") issued a Notice of Proposed Rulemaking ("NPRM") that, if implemented, would require maritime transportation system ("MTS") operators to institute several minimum cybersecurity performance standards. Those measures include supply chain requirements, such as considering cybersecurity capabilities in selecting vendors, establishing procedures for information sharing and notifying relevant parties, and monitoring third-party connections.[12]

The USCG NPRM follows a well-documented trend of voluntary supply chain and cybersecurity frameworks being replaced with regulatory mandates as U.S. federal agencies issue an increasing number of regulations that obligate covered entities to

---

[10] For more information regarding the UFLPA, *see Debevoise ESG Weekly Update – July 26, 2023* ("U.S.: SEC Asks Chinese Companies to Disclose Uyghur Forced Labor Ties"), *available at* https://www.debevoise.com/insights/publications/2023/07/26-esg-weekly-update; Debevoise ESG Weekly Update – July 7, 2023 ("U.S.: Congress Publishes Interim Findings on Forced Labor Investigation of Chinese Shopping Sites"), *available at* https://www.debevoise.com/insights/publications/2023/07/07-esg-weekly-update; *Debevoise ESG Weekly Update – July 13, 2022* ("Uyghur Forced Labor Prevention Act Goes Into Effect"), *available at* https://www.debevoise.com/insights/publications/2022/07/13-esg-weekly-update; New Sanctions on China: The Uyghur Forced Labor Prevention Act and Further Chinese Company Designations, debevoise.com (Dec. 21, 2021), *available at* https://www.debevoise.com/insights/publications/2021/12/new-us-sanctions-on-china-the-uyghur-forced-labor.

[11] *See FACT SHEET: DHS Moves to Improve Supply Chain Resilience and Cybersecurity Within Our Maritime Critical Infrastructure*, dhs.gov (Feb. 21, 2024), *available at* https://www.dhs.gov/news/2024/02/21/fact-sheet-dhs-moves-improve-supply-chain-resilience-and-cybersecurity-within-our.

[12] *See Cybersecurity in the Marine Transportation System*, 89 F.R. 13404 (Feb. 22, 2024) § 101.650(F).

adopt baseline supply chain and cybersecurity measures. MTS operators should, either independently or through industry associations, consider commenting on the USCG's NPRM and look for additional opportunities to engage with the rulemaking process.

Congressional Concern Over Applications Controlled by Foreign Adversaries

Congress remains active in scrutinizing supply chain security in several of the preceding domains. In addition to its efforts to increase enforcement of the UFLPA, on March 5, 2024, the Chair and Ranking Member of the Committee introduced bipartisan legislation that, among other things, would prohibit the availability in app stores and web hosting services of applications that are alleged to be controlled by a foreign adversary, including TikTok.[13] Although ostensibly intended to obligate ByteDance to divest TikTok, the legislation, if enacted, would require app stores and web hosting services to diligence applications before making them available on their platforms. It could also have far-reaching implications for companies that rely on such applications in their supply chains (such as for implementing or overseeing operations). Congress's growing concern regarding the potential national security implications of Chinese applications and other ICTS will continue to drive congressional interest and possible future punitive measures.

Key Takeaways

- Federal agencies are leveraging more tools and regulatory authorities than ever to compel companies to monitor their supply chains for national security concerns and other forms of risk. Agencies are acting across several industry sectors, with DOJ, DOC, DOD, and DHS, among others, initiating regulatory and enforcement actions.

- Affected parties should monitor these developments and ensure that their supply chain security programs are properly tailored to their respective risk exposure to each of the federal government's recent supply chain initiatives.

* * *

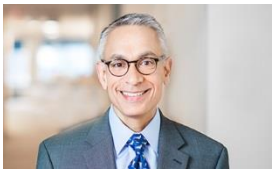
Please do not hesitate to contact us with any questions.

---

[13] *See* Protecting Americans from Foreign Adversary Controlled Applications Act, 118th Congress (2024).

Catherine Amirfar
Partner, New York
+1 212 909 7423
camirfar@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com



Satish M. Kini
Partner, Washington, D.C.
+1 202 383 8190
smkini@debevoise.com

Erez Liebermann
Partner, New York.
+1 212 909 6224
eliebermann@debevoise.com

Rick Sofield
Partner, Washington, D.C.
+1 202 383 8054
rcsofield@debevoise.com

Robert T. Dura
Counsel, Washington, D.C.
+1 202 383 8247
rdura@debevoise.com

Gabriel Kohan
Associate, Washington, D.C.
+1 202 383 8036
gakohan@debevoise.com

Stephanie D. Thomas
Associate, New York
+1 212 909 6535
sdthomas@debevoise.com