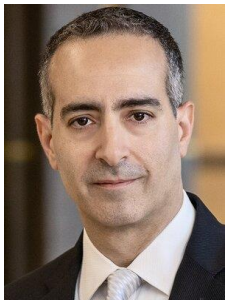
LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Republican Trifecta Amplifies Risks For Cos. In 3 Key Areas

By **Amanda Robinson, David Plotinsky and Emily Ahdieh** (January 13, 2025, 3:47 PM EST)


Amanda Robinson


David Plotinsky


Emily Ahdieh

As the 119th Congress commences under Republican control, and President-elect Donald Trump once again assumes office on Jan. 20, the private sector should brace for heightened scrutiny across a range of critical issues.

With a Republican trifecta, Congress is less incentivized to take an aggressive approach to reviewing, monitoring and supervising executive branch activities, and, instead, will turn its focus to the private sector.

Expected coordination between Congress and the executive branch raises the stakes for companies, potentially exposing them to simultaneous criminal, civil administrative and congressional investigations.

This environment will likely amplify risks in various areas, including several national security-related areas that benefit from notable bipartisan support: (1) supply chain risks, particularly in the technology and pharmaceutical industries; (2) government contracting; and (3) cross-border investment.

**Technology and Pharmaceutical Supply Chain Risks**

National security remains one of the few bipartisan issues before Congress. Both legislative and executive efforts have increasingly focused on safeguarding the U.S.' critical supply chains.

Under a Republican-led government, there will likely be an intensified focus on supply chain vulnerabilities, particularly in the technology and pharmaceutical sectors.

Recent supply chain disruptions, coupled with geopolitical tensions, have highlighted the U.S.' dependency on foreign sources, including China, for critical components in technology and pharmaceuticals.

Congressional scrutiny is likely to draw from legislative and executive efforts initiated during the first Trump administration, which continued during the 117th and 118th Congresses and the Biden administration.

Under the first Trump administration, foundational measures like the Strengthening and Enhancing

Cyber-Capabilities by Utilizing Risk Exposure, or Secure, Technology Act were passed. And in May 2019, Executive Order No. 13873 on safeguarding IT and communication technology supply chains was issued to identify and address supply chain threats to sensitive technology systems.

These measures, among others, empowered governmental bodies like the Federal Acquisition Security Council and the U.S. Department of Commerce to scrutinize and mitigate supply chain risks, particularly those with touchpoints to U.S. foreign adversaries, such as China and Russia.

Those frameworks will continue to shape rulemaking, investigations and enforcement actions targeting supply chain security during Trump's second term.

More recently, the FASC Improvement Act was proposed in September 2024 and is currently pending in the U.S. Senate. The bill seeks to further empower FASC. The legislation would expand FASC's authority by enabling it to take more decisive action against companies that present supply chain risks to the U.S. government through their nexus to foreign adversaries.

The bill has bipartisan backing and was passed overwhelmingly in the U.S. House of Representatives. A version of the bill was subsequently approved by the Senate Committee on Homeland Security and Governmental Affairs before being sent to the Senate floor for consideration.

The bill was not included in the fiscal year 2025 National Defense Authorization Act, which sets the stage for the 119th Congress to push the legislation over the finish line.

Should the FASC Improvement Act become law, it would enhance the federal government's ability to identify and mitigate supply chain threats. For example, the FASC Improvement Act authorizes Congress to designate sources of concern that FASC must investigate, and further empowers FASC to directly issue binding removal and exclusion orders when instructed to do so by Congress.

This new authority given to Congress and FASC under the FASC Improvement Act would likely lead to more investigations and enforcement actions against companies with connections to foreign adversary countries like China or Russia.

In addition, the pharmaceutical industry remains vulnerable to heightened scrutiny, particularly because of the U.S.' reliance on active pharmaceutical ingredients sourced from China. Republicans have explicitly highlighted the national security and supply chain risks posed by the pharmaceutical industry's reliance on Chinese-sourced active pharmaceutical ingredients.

In 2023, Sen. Marco Rubio, R-Fla., introduced the Further Strengthening America's Supply Chains and National Security Act to combat America's dependence on China for pharmaceuticals and resulting drug shortages.

Similarly, Sen. Tom Cotton, R-Ark., and former Rep. Mike Gallagher, R-Wis., then-chair of the House Select Committee on the Chinese Communist Party — introduced the Protecting Our Pharmaceutical Supply Chain from China Act, which would require the federal government to maintain a registry of some drugs manufactured overseas, and would prohibit federal health programs from purchasing drugs with Chinese ingredients.

While neither of those proposed laws passed during the Biden administration, the upcoming Republican trifecta is likely to remain focused on the pharmaceutical industry and the security of its supply chains.

Forced labor also looms as a critical issue resulting from the U.S.' reliance on foreign supply chains. Existing legislation, such as the Uyghur Forced Labor Prevention Act, has already restricted imports tied to forced labor. A unified Republican-controlled government could lead to expanded enforcement or new legislation targeting broader supply chain practices.

The UFLPA already imposes a presumption of forced labor for goods originating in the Xinjiang region, shifting the burden of proof to companies. A Republican trifecta can be expected to legislate further; conduct oversight investigations into allegations of forced labor; and likely encourage the Trump administration to expand the UFLPA entity list and to consider expanding the list of high-priority sectors, where forced labor concerns persist.[1]

At the executive level, the U.S. Department of Homeland Security, and the U.S. Customs and Border Protection agency within it, have been increasingly active in enforcing import bans under forced labor laws.

Republican leaders have been vocal about combating forced labor and supply chain vulnerabilities. Rubio, currently poised to head the U.S. Department of State in Trump's upcoming administration, co-sponsored the UFLPA. Rubio and other prominent Republican representatives have sent letters to the White House proposing the addition of certain Chinese companies to the UFLPA entity list. However, these companies have not yet been added by the Biden administration.

Under a unified Republican-controlled government, there may be more aggressive UFLPA entity designations, and consequently, an increase in legal challenges of those designations.

In addition, Rep. Elise Stefanik, R-N.Y., who is Trump's nominee for ambassador to the United Nations, has similarly called for robust congressional oversight to ensure that American supply chains are free from forced labor abuses.

Rubio and Stefanik's expected leadership in the upcoming administration will likely drive legislative and investigative priorities, including a focus on forced labor.

As Republican legislators zero in on supply chain security, organizations that fail to adequately vet their supply chains are vulnerable to simultaneous congressional inquiries and executive branch enforcement actions. Enforcement actions may include import bans, penalties for forced labor violations, exclusion orders and licensing revocations.

**Government Contracting Scrutiny**

Government contractors should gear up for continued and elevated congressional oversight of procurement processes and performance under federal contracts.

FASC's current role in monitoring supply chain security in the information technology sector is a key example, but government contractors across all industries may face inquiries into compliance with "Buy American" rules and national security-related mandates.

In 2017, Trump issued Executive Order No. 13788, titled "Buy American and Hire American," which sought to increase the enforcement of laws relating to domestic preferences for government procurement.

This executive order was revoked and replaced in 2021 by Biden's Executive Order No. 14005, which directs federal government agencies to maximize the use of goods, products and materials produced in, and services offered in, the U.S.

Both executive orders sought to tighten "Made in America" laws, including the Buy American Act, to ensure a greater proportion of federal procurement dollars are spent on American-made products.

With Trump back in office, and the bipartisan interest in investing in U.S.-made products, government contractors should expect federal procurement policies and enforcement efforts that continue — or further — the current trajectory.[2]

This scrutiny over federal procurement is likely to continue and increase with the next administration's intersectional concern with securing federal supply chains and ensuring adequate cybersecurity.

In his previous administration, Trump accelerated regulations aimed at protecting information from cyber bad actors and foreign adversaries through the Cybersecurity Maturity Model Certification, or CMMC, program.

The CMMC program — which builds on existing cybersecurity requirements for defense contractors, while also introducing new certification and review obligations — began under the previous Trump administration and was continued by the Biden administration.

The long process to issue regulations that implement the CMMC program is now in its final stages, and will likely continue during Trump's upcoming administration.

The CMMC program supports Trump's policy focus by seeking to prevent adversaries like China from successfully accessing and exfiltrating critical information held by the U.S. government and federal contractors.

Accordingly, compliance with cybersecurity requirements and ensuring supply chain resilience will continue to be critical for federal prime contractors, subcontractors and their suppliers.

Supply chain security probes by FASC, and compliance enforcement investigations by the U.S. Department of Defense and other contracting agencies, could further complicate a government contractor's legal and operational risks.

Congress may enhance measures put into place by the Secure Technology Act by pushing for additional reforms to strengthen government procurement processes. Potential measures include enhanced cybersecurity requirements for contractors, stricter disclosure mandates for supply chain practices, and expanded debarment standards for those found noncompliant.

In alignment with the previous Trump administration's cybersecurity initiatives, a Republican Congress may work with the incoming administration to further enhance the cybersecurity requirements and compliance enforcement efforts for government contractors that support all agencies.

It is essential for companies contracting with the government to maintain proactive compliance measures and robust internal monitoring systems in order to mitigate risks, especially in light of potentially increased scrutiny by the upcoming administration.

**Cross-Border Investment**

The 118th Congress — in particular, the House Select Committee on Strategic Competition between the U.S. and the Chinese Communist Party — devoted significant attention to cross-border investment involving China,[3] and that focus may continue in the next Congress. That focus includes both foreign direct investment by China in the U.S., and outbound investment by U.S. investors in China.

The upcoming Republican-controlled Congress may push for expanded regulations governing outbound investments in foreign entities, especially those in adversarial nations like China, Russia and Iran.

Restrictions on outbound investments are already in place as a result of Biden's Executive Order No. 14105 on U.S. national security technology investments in countries of concern, and related U.S. Department of the Treasury regulations.

Executive Order No. 14105 invoked the International Emergency Economic Powers Act and the National Emergencies Act to prohibit or restrict certain U.S. investments in China on the basis of national security.

In October 2024, the Treasury Department issued final regulations restricting certain artificial intelligence, semiconductor and quantum computing investments by U.S. persons in Chinese companies. These regulations' prohibitions and reporting requirements went into effect on Jan. 2.

Additionally, while Speaker of the House Mike Johnson, R-La., was reportedly pushing Congress to include its own outbound investment restrictions in the fiscal year 2025 National Defense Authorization Act, the restrictions did not make it into the final legislation.

It remains unclear if outbound investment legislation can overcome long-standing disagreements, particularly between the House Foreign Affairs Committee and the House Financial Services Committee.

The new Congress may pick outbound investment legislation back up, possibly by resurfacing legislation such as the National Critical Capabilities Defense Act, introduced in the 118th Congress. In some respects, that act was broader than Executive Order No. 14105 and the related regulations.

With respect to foreign direct investment in the U.S., Congress may push to broaden existing laws, such as the Foreign Investment Risk Review Modernization Act, which previously updated the role of the Committee on Foreign Investment in the United States. Various legislation has been introduced in recent months to further expand CFIUS' authority.[4]

In addition to formal oversight by Congress, individual members of Congress may attempt to influence CFIUS' review of certain transactions by advocating to the committee, or by publicly commenting on transactions and raising concerns about their effects.[5]

For example, during the review of Nippon Steel Corp.'s proposed acquisition of U.S. Steel Corp., several members of Congress — including Republican Sens. JD Vance, R-Ohio; Josh Hawley, R-Mo.; and Rubio; as well as Democratic Sens. Sherrod Brown, D-Ohio; John Fetterman, D-Pa.; and Bob Casey, D-Pa.; and Independent Sen. Joe Manchin, I-W.V. — raised concerns about the deal's impact on the domestic steel supply chain and its strategic implications for national security.

However, other members of Congress, including Republican Reps. Bill Huizenga, R-Mich.; Andy Barr, R-

Ky.; Dan Meuser, R-Pa.; and John Rose, R-Tenn., expressed concern that CFIUS might block the transaction for improper political reasons. And in September 2024, they sent a letter to Treasury Secretary Janet Yellen requesting the preservation of all documents related to the transaction, further underscoring the close examination and political sensitivity surrounding the deal and signaling that further oversight in the form of a congressional investigation may be forthcoming.

Ultimately, CFIUS failed to reach a consensus about whether Nippon Steel should be allowed to buy U.S. Steel, and on Jan. 3, Biden issued an order blocking the transaction. Both Nippon Steel and U.S. Steel have filed lawsuits in response to the order, alleging government wrongdoing that may overlap with some of the expressed congressional concerns about politicization of the process.

Public comments from individual Congress members can bring certain considerations to the forefront of CFIUS review, such as national security and supply chain concerns.

These concerns will be important to this new Republican-controlled Congress. Therefore, companies seeking to enter into transactions subject to CFIUS review should factor in whether a transaction would be likely to generate congressional interest, and any impact that might have.

**Key Takeaways and Conclusion**

The expected alignment between Congress and the executive branch will amplify criminal, civil administrative, and congressional regulation of and enforcement against companies involved in federal supply chains, government contracting and foreign investment.

To mitigate these risks, organizations should take the following measures.

***Proactively assess vulnerabilities.***

Companies should conduct thorough audits of supply chain practices, government contracts and foreign investment portfolios to identify and address potential areas of concern.

***Enhance compliance programs.***

Companies should strengthen their compliance programs to address forced labor, cybersecurity and federal procurement requirements. They must also ensure that disclosures to federal agencies are accurate and complete.

***Develop crisis management plans.***

Companies should prepare for simultaneous congressional inquiries and executive branch investigations by developing coordinated response strategies.

***Monitor legislative developments.***

Finally, companies should stay informed of proposed legislation and enforcement trends to anticipate and adapt to evolving regulatory requirements.

**Conclusion**

Vigilance and preparedness are essential for businesses across industries. With national security as a driving force, and with a Republican-controlled Congress focused on the private sector, both government contractors and other technology and investment companies must prioritize compliance and risk mitigation to avoid becoming targets in this multifaceted regulatory environment.

---

*Amanda B. Robinson is a partner and co-head of the congressional investigations practice at Morgan Lewis & Bockius LLP. She previously served as associate counsel and presidential management fellow at the U.S. Department of Health and Human Services' Office of Inspector General.*

*David Plotinsky is a partner and co-head of the congressional investigations practice at Morgan Lewis. He previously served as acting chief of the U.S. Department of Justice's Foreign Investment Review section, as associate deputy general counsel in the Office of the Director of National Intelligence's Office of General Counsel, and as assistant counsel in the U.S. House of Representatives Office of General Counsel.*

*Emily Ahdieh is an associate at the firm.*



[1] Additionally, allegations of forced labor will also likely be used to support broader legislative efforts such as ending the de minimis tariff exemption by Chinese shippers to possibly revoking permanent normal trade relations (PNTR) with China.

[2] For example, under the Biden Administration's Make PPE in America Act, manufacturers of certain personal protective equipment sold to the US government were required to manufacture the equipment in the United States. Under the upcoming Trump Administration, government contractors that sell critical supplies to the US government could expect regulatory actions requiring their products and components be fully manufactured in the United States.

[3] For example, the 118th Congress investigated investments in Chinese technology companies made by US venture capital firms. The investigation was led by the House CCP committee, which released a report summarizing the investigation and concluded that US venture capital firms invested billions into the Chinese government's critical technology companies, including many companies that aid the Chinese military and surveillance state. The House CCP also conducted an investigation into the US financial industry and released a report finding that US index providers and asset managers, on an industry-wide basis, facilitated the investment of more than $6.5 billion to Chinese companies that the US government has red-flagged or blacklisted for advancing the Chinese government's military capabilities or supporting its human rights abuses.

[4] For example, the House recently passed the Protecting American Agriculture from Foreign Adversaries Act of 2024. This bill would increase oversight and restrict foreign investment in US agriculture by mandating that CFIUS review transactions involving foreign investments in US agriculture, including farmland.

[5] For example, in the CFIUS review of CSG's acquisition of the ammunition business of Vista Outdoor, various lawmakers opposed the transaction due to supply assurance concerns and alleged ties by CSG

ties to Russia. Members of Congress from both political parties released letters highlighting their national security concerns, including then-Senator and current Vice President-elect JD Vance. Ultimately, however, CFIUS approved the transaction.