Nordic Newsletter

January 2025

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

Editors' Note

Hi friends and colleagues,

Wishing you a Happy New Year! We are excited to release a new issue of Covington & Burling's Nordic Newsletter.

In this edition, we compiled articles published by Covington lawyers discussing, among others:

- recent developments in the US artificial intelligence regulatory framework in the context of national security,
- likely trends in U.S. tech and media regulation under the Trump administration,
- recent enforcement actions of the SEC's whistleblower rules concerning employee agreements,
- the new US Hart-Scott-Rodino (HSR) Act competition notification requirements,
- recent EU developments on the GDPR's "legitimate interests" legal basis, and
- a comparison of UK and U.S. trends on employee non-compete clauses.

In this issue, we are delighted to introduce you to our partner Einar Stole. Einar is a patent litigator based in our DC office. Einar is a core member of our Nordic Initiative and has extensive professional and personal experience in the region. If you are running out of podcasts, feel free to check our recent webinars discussing U.S. deal trends relevant to Nordic businesses, as well as tips on how to navigate the trade controls landscape in the U.S., UK, and EU, and sanctions and export controls impacting doing business with China and Russia.

We are grateful for our clients continued trust in Covington. We reiterate our commitment to the Nordic market and will continue to work closely with our Nordic clients in supporting their legal needs across jurisdictions and practice areas. Thanks for reading thus far! We hope you find these materials useful, and we look forward to opportunities to connect in 2025!

Barbara, Uri and Jared

Uri Doron
M&A, Private Equity
Partner, New York
+1 212 841 1042
UDoron@cov.com

Jared Manes
M&A, Private Equity
Partner, New York
+1 212 841 1054
JManes@cov.com

Barbara Asiain
M&A, Private Equity
Associate, New York
+1 212 841 1053
BAsiain@cov.com

Contents

Meet the Nordic Initiative:
Einar Stole

Who is Einar Stole?

I grew up in Seattle, Washington in a Norwegian-speaking home. Both my parents emigrated from Norway, and I have spent significant time in Norway with family and friends. I am now based in Covington's Washington, D.C. office where I focus on patent litigation for our life sciences and pharmaceutical clients. I began as a scientist before I transitioned to a role as a U.S. patent examiner and then to private practice with a focus on litigation.

Tell us about your legal practice...

I advise our life sciences and pharmaceutical clients on strategies for obtaining, enforcing and defending patent rights. I also represent clients in litigation in U.S. Courts and in proceedings before the USPTO. I have counseled clients in the Nordics for over 20 years.

Trends and recent developments in the region?

Nordic clients engage in global markets. Recent developments in U.S. law relating to double patenting (and terminal disclaimers) and induced infringement impact strategies for obtaining and enforcing patent rights in the U.S. and globally.

Your go-to Nordic restaurant / dish

Since childhood, my favorite meal is fårikål (lamb & cabbage).

Favorite Nordic movie / music band

Åge Aleksandersen.

Ideal Nordic holiday

Hiking between huts (hytter) in the mountains of Norway.

Licorice or kanelbulle?

Lakris. Of course!

Events

NORDIC WEBINAR SERIES:

Navigating Transatlantic deals between the Nordics and the U.S.

The U.S. presents significant investment and M&A opportunities for Nordic companies. Our team of leading experts advise Nordic companies daily on structuring transactions to successfully achieve their strategic objectives.

This webinar covered recent M&A trends, tips on how to navigate the current U.S. regulatory framework, and opportunities to leverage U.S. incentives for innovation and growth. It will be of interest to Nordic companies and investors considering transatlantic deals in the short- to medium term.

Watch Here

Topics Include:

- Market trends and legal developments impacting Nordic buyers in the U.S. market
- Enhancement of CFIUS's Enforcement Authorities: what is motivating the U.S. government in how they apply screening of foreign investments, and what trends are we seeing?
- Acquiring distressed businesses or their assets in the U.S., including through 363 sales under the Bankruptcy Code
- U.S. government incentives as a means of combining U.S. capital with Nordic innovation

Heather Finstuen
CFIUS
Partner, Washington
+1 202 662 5823
HFinstuen@cov.com

Abigail O'Brient
Restructuring and Bankruptcy
Partner, Los Angeles
+1 424 332 4826
AOBrient@cov.com

Johan Dagergard
Corporate / M&A
Special Counsel, London
+44 20 7067 2341
JDagergard@cov.com

Mike Wagner
Government Contracts
Partner, Washington
+1 202 662 5496
MWagner@cov.com

NORDIC WEBINAR SERIES:

Navigating the International Trade Controls Landscape: Considerations for Nordic Businesses

Companies are facing increasingly complex and expanding economic sanctions and export controls, as well as an unprecedented rise in trade controls enforcement by the U.S. and other governments. As a result, companies operating internationally must navigate greater compliance and enforcement risks than previously. Our team of leading experts in the U.S., EU, and UK advise Nordic companies through the most complex regulatory and compliance issues, to aid them in achieving their strategic objectives.

This webinar covered tips on how to navigate the trade controls landscape following the U.S. election, the current enforcement environment in the UK, EU and the U.S., and sanctions and export controls impacting doing business with China and Russia. It will be of interest to Nordic companies seeking multijurisdictional guidance on the trade controls compliance and enforcement environment.

Watch Here

Topics Include:

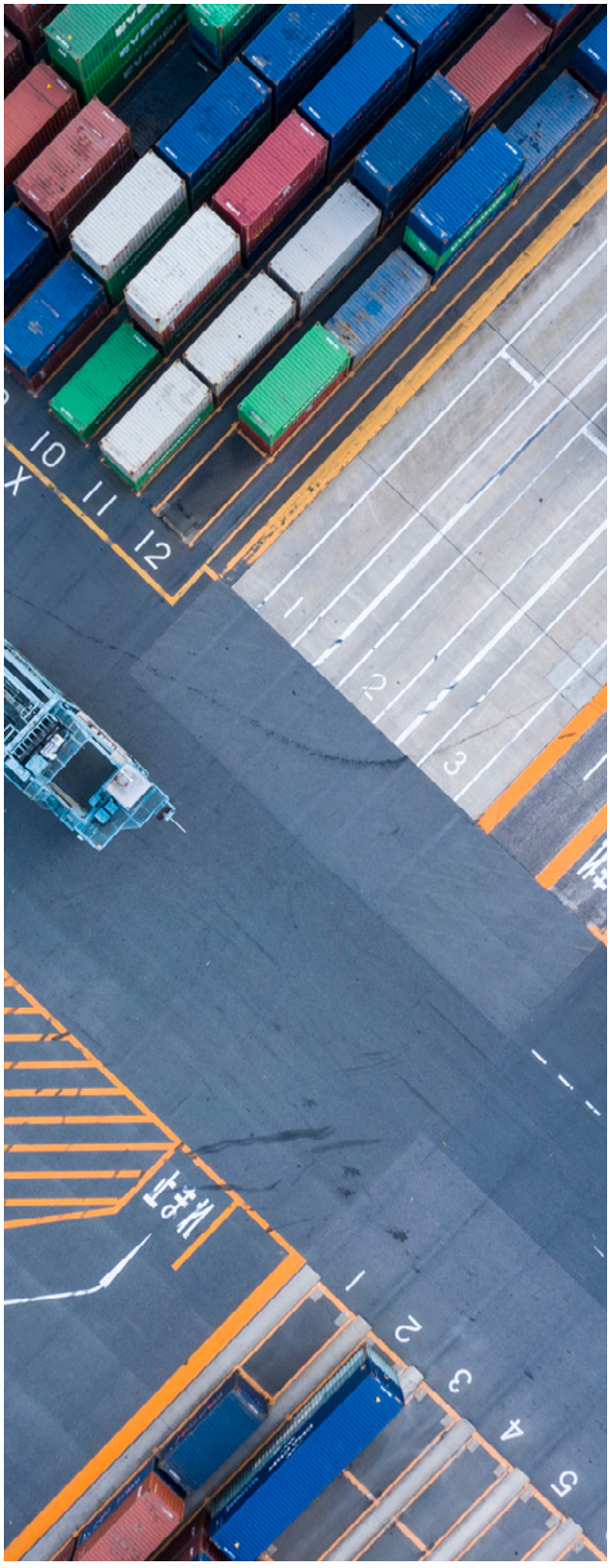
- Global enforcement trends and environment
- Trade Controls landscape post-U.S. election
- Sanctions and export controls affecting China and Russia

David Lorello
International Trade
Partner, London
+44 20 7067 2012
DLorello@cov.com

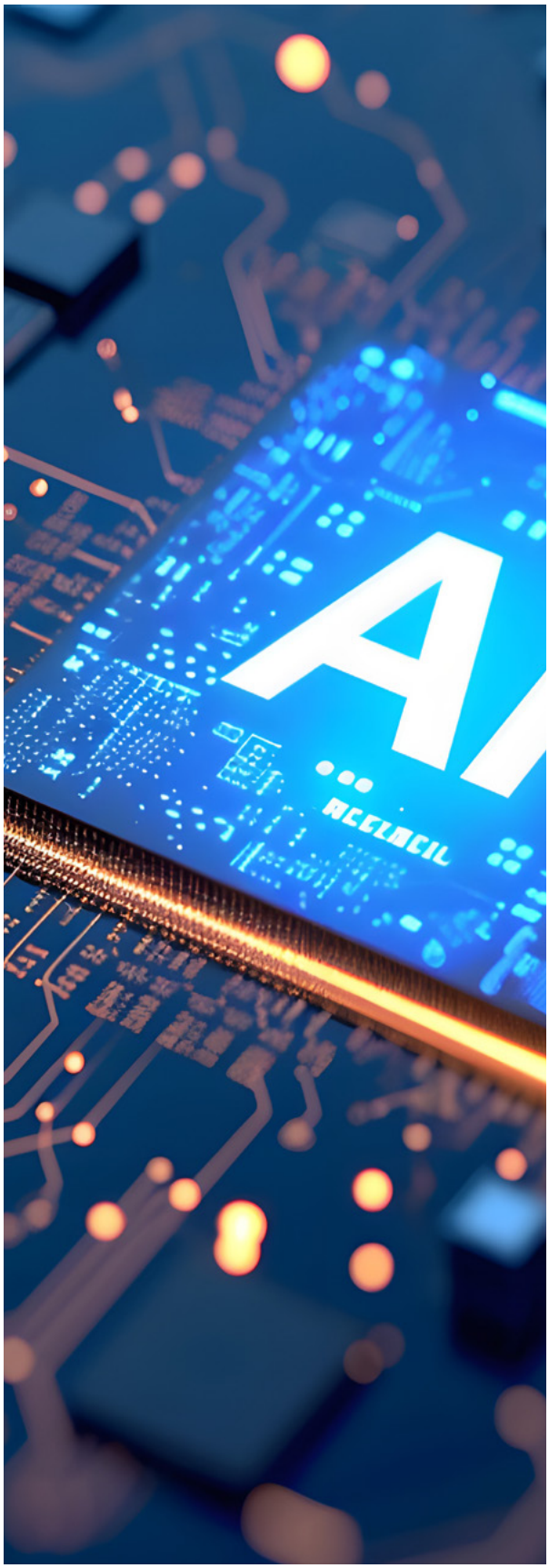
Lisa Ann Johnson
International Trade
Associate, Washington
+1 202 662 5928
LiaJohnson@cov.com

Joshua Williams
Trade Controls
Enforcement
Partner, Washington
+1 202 662 5618
JnWilliams@cov.com

Emanuel Ghebregergis
International Trade/White Collar
Defense and Investigations
Associate, Frankfurt
+49 69 768063 359
EGhebregergis@cov.com



White House Issues National Security Memorandum on Artificial Intelligence ("AI")



On October 24, 2024, the White House issued a National Security Memorandum on the use of AI models and AI-enabled technologies in national security systems and for military or intelligence purposes ("AI NSM"). The AI NSM fulfills § 4.8 of the White House's October 2023 Executive Order 14110 ("AI Executive Order"), which requires White House national security officials to develop and submit an AI NSM to guide adoption of AI capabilities in support of U.S. national security and address potential uses of AI by adversaries and other foreign actors. The AI NSM is the latest in a series of recent executive branch actions to implement the AI Executive Order, including the Office of Management and Budget's ("OMB's") March 2024 Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* ("March 2024 OMB Memo"), which we have previously covered here, and October 2024 Memorandum M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government* ("October 2024 OMB Memo"), summarized in our recent client alert here.

Acknowledging that the current "paradigm shift within the AI field . . . has occurred mostly outside of Government," the AI NSM directs the U.S. Government to "act with responsible speed and in partnership with industry, civil society, and academia to make use of AI capabilities in service of the national security mission," while ensuring "the safety, security, and trustworthiness of American AI innovation writ large." Failure to act, the AI NSM warns, "risks losing ground to strategic competitors," undermining U.S. foreign policy objectives, and "erod[ing] safety, human rights, and democratic norms worldwide."

To that end, the AI NSM outlines the goals of: (1) directing actions to strengthen and protect the U.S. AI ecosystem; (2) improving the safety, security, and trustworthiness of AI systems developed and used in the U.S.; (3) enhancing the U.S. Government's effective adoption of AI in service of the national security mission; and (4) minimizing the misuse of AI worldwide.

The AI NSM's requirements apply to elements of the Intelligence Community, and to any agency (other than the Executive Office of the

President, the Government Accountability Office, or the Federal Election Commission) that uses AI as a component of a "national security system." A national security system is generally defined by the AI NSM to mean an information system that involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment integral to weapons or weapons systems, or the fulfillment of military or intelligence missions, or an information system that is classified in the interest of national defense or foreign policy by Executive Order or an Act of Congress. The AI NSM will therefore directly impact companies that support these systems, as it outlines a number of requirements in that regard. The AI NSM will also likely have broader impacts outside of the government acquisition context, including with regard to the development and testing of AI models and the Government's investments in and support of emerging AI technologies.

Following the 2024 U.S. elections, the incoming Trump Administration, Republican-controlled Senate, and likely Republican-controlled House are certain to impact the implementation of the AI NSM and the Biden Administration's other AI initiatives. While President-elect Trump has stated that he will rescind the 2023 AI Executive Order, it remains to be seen whether the AI NSM will be rescinded, replaced, or maintained. Notably, in 2019, the first Trump Administration issued Executive Order 13859, summarized in our blog post here, which directed the OMB to establish guidance on federal agency use of AI and called for an "action plan" for protecting U.S. AI technologies critical to U.S. national security interests from foreign competitors and adversaries. These and other prior Trump Administration AI actions, including the National AI Initiative Act, AI in Government Act, and a 2020 Executive Order that set out principles for agency uses of AI, suggest that there may be some continuities between the two administrations' approaches to AI policy.

1 U.S. AISI Frontier AI Safety Testing and Proactive AI Testing Infrastructure

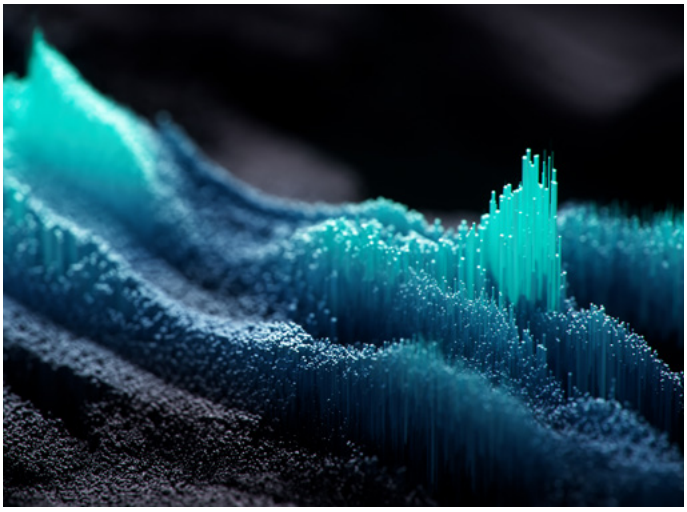
Section 3.3 of the AI NSM outlines proactive safety "testing infrastructure" and standards to assess AI risks while "preserving the United States AI leadership." This section directs the Department of Commerce ("Commerce"), acting through NIST's U.S. AI Safety Institute ("AISI") as the primary U.S. point of contact with private sector AI developers, to establish voluntary, unclassified, pre-deployment safety testing of frontier AI models. This safety testing must assess risks related to cybersecurity, biosecurity, chemical weapons, system autonomy, human rights, civil rights, and civil liberties. However, according to § 3.3(c), this capability does not extend to assessments of nuclear risks, which are delegated to the Department of Energy ("DOE").

AISI's frontier AI safety testing infrastructure does not preclude agencies from performing their own evaluations of AI systems, including tests performed before systems are released to the public and for the purposes of evaluating suitability for procurement. Notably, AISI's safety testing responsibilities do not apply to AI systems used for national security purposes. As discussed below, testing and evaluation of AI systems in national security contexts are governed by the AI Framework established in § 4.2(e).

A. Preliminary Testing of Frontier AI Models

Subject to private sector cooperation, AISI must pursue voluntary preliminary testing of at least two frontier AI models prior to and following their public deployment or release, in order to evaluate national security threats. The testing must assess model capabilities to "aid offensive cyber operations, accelerate development of biological and/or chemical weapons, autonomously carry out malicious behavior, automate development and deployment of other models with such capabilities, and give rise to other risks identified by AISI." AISI must share feedback on risks and mitigations with the Assistant to the President for National Security Affairs ("APNSA"), interagency counterparts, and the model developers prior to deployment.

Relatedly, in August 2024, AISI announced "first-of-their kind" Memoranda of Understanding with two U.S. AI companies to collaborate on AI safety research, testing, and evaluation. The agreements allow AISI to "receive access to major new models from each company prior to and following their public release," with the goal of enabling "collaborative research on how to evaluate capabilities and safety risk," including risk mitigation methods. AISI intends to collaborate with the UK AI Safety Institute to provide feedback on model safety improvements.



B. General Guidance on Testing and Risk Management

AISI must issue guidance for AI developers on testing, evaluating, and managing risks of dual-use foundation models, "building on guidelines issued pursuant to subsection 4.1(a) of Executive Order 14110." In July 2024, NIST took initial steps to fulfill § 4.1(a) with the release of the initial public draft guidelines on "Managing Misuse Risks for Dual-Use Foundation Models." The AISI testing guidance required by the AI NSM must build on this guidance by addressing: (1) how to measure capabilities relevant to biological and chemical weapons or automated offensive cyber operations, (2) how to address societal risks like misuse to harass or impersonate others, (3) how to develop mitigation measures to prevent malicious or improper use, (4) how to test efficacy of safety and security mitigations, and (5) how to apply risk management practices throughout development and deployment lifecycle. The National Security Agency ("NSA"), DOE, and the Department of Homeland Security ("DHS") are instructed to perform "complementary voluntary classified testing in appropriate areas of expertise," as discussed in Part II below.

AISI is also required to recommend benchmarks or other methods for assessing AI capabilities and limitations in science, math, code generation, general reasoning, and other categories of activity AISI deems relevant to "assessing general-purpose capabilities that may affect national security and public safety." Additionally, the AI NSM directs AISI to serve as the primary point of contact for communications with developers, including communicating determinations that an AI developer's model has capabilities that could harm public safety "significantly," as well as any recommendations for risk mitigation.

2 Agency Sector-Specific AI Testing for Cyber, Nuclear, and Radiological Risks

A. Sector-Specific AI Evaluations for Cyber, Nuclear, and Radiological Risks

Section 3.3(f) of the AI NSM requires agencies to collaborate with Commerce, acting through AISI, to implement evaluations of AI systems specific to cyber, nuclear, and radiological risks. All agencies that "conduct or fund safety testing and evaluation of AI systems" are required to share the results with AISI within 30 days of completion, consistent with protections for classified and controlled information.

Additionally, the AI NSM directs the NSA, through its AI Security Center ("AISC") and in coordination with AISI, to develop the capability to perform "rapid, systematic, classified testing" of AI models' potential to "detect, generate, and/or exacerbate offensive cyber threats." These evaluations must be designed to assess the degree to which AI systems, if misused, could "accelerate offensive cyber operations."

DOE is similarly directed to develop, in coordination with AISI and NSA, capabilities for rapid, systematic testing of AI models' potential to generate or exacerbate nuclear and radiological risks. This initiative must involve creating and maintaining infrastructure for both classified and unclassified testing, including the use of "restricted data and relevant classified threat information," automated evaluation processes, an interface for human-led red-teaming, and secure mechanisms for transferring government and proprietary models.

As part of this initiative, DOE is required to complete initial evaluations of an AI model's nuclear and radiological risks within 30 days of the model's availability and to submit, at least annually, a report to the President through APNSA that includes evaluation findings, recommendations for corrective actions, and an assessment of the adequacy of the tools and methods used to inform evaluations.

B. Classified Evaluations to Reduce Chemical and Biological AI Risks

Section 3.3(g) of the AI NSM directs the U.S. Government to reduce chemical and biological risks that could emerge from AI through "classified evaluations of advanced AI models' capacity to generate or exacerbate deliberate chemical and biological threats."

As part of this initiative, DOE, DHS, and AISI, in consultation with the Department of Defense ("DOD") and other relevant agencies, are required to develop a roadmap for future classified evaluations of advanced AI models, shared with APNSA. This roadmap must outline the "scope, scale, and priority of classified evaluations," ensure proper safeguards, and maintain secure testing of sensitive and/or classified information. It must also establish sustainable methods for implementing evaluation methodologies.

Furthermore, DOE is required to "establish a pilot project to provide expertise, infrastructure, and facilities capable of conducting classified tests" for chemical and biological AI risks.

Upon publication of AISI's biological and chemical safety guidance, all agencies developing relevant dual-use foundation AI models that are (1) made available to the public and (2) significantly trained on biological or chemical data must incorporate this guidance into their practices.

In addition, DOD, the Department of Health and Human Services ("HHS"), DOE, DHS, the National Science Foundation ("NSF"), and other relevant agencies involved in the development of AI systems substantially trained on biological and chemical data are instructed to prioritize biosafety and biosecurity by:

- Developing tools to evaluate virtual chemical/biological research and technologies;
- Creating algorithms to monitor and screen synthesized nucleic acids;
- Building secure and reliable software frameworks to support new biotechnologies;
- Screening full data streams or orders from cloud-based labs and bio-manufacturing facilities, and
- Developing strategies to mitigate risks, including the creation of medical countermeasures.

Finally, NSF, in coordination with DOD, AISI, HHS, DOE, the Office of Science and Technology Policy ("OSTP"), and other relevant agencies, must convene academic research institutions and scientific publishers to develop "voluntary best practices and standards for publishing computational biological and chemical models, data sets, and approaches." This effort aims to address AI applications "that could contribute to the production of knowledge, information, technologies, and products that could be misused to cause harm," in line with activities outlined in the 2023 AI Executive Order.

3 National Security AI Risk Management Framework

To provide appropriate safeguards, accountability, and control in the use of AI for national security, § 4.2 of the AI NSM establishes a set of AI governance and risk management practices for national security uses. These practices, outlined in the AI NSM's companion "Framework to Advance AI Governance and Risk Management in National Security" ("AI Framework"), are intended to "serve as a national security-focused counterpart" to the March 2024 OMB Memo and its minimum risk management practices for rights-impacting and safety-impacting AI outside the national security context. Accordingly, these practices apply to agencies that use AI as part of a national security system. Although there are similarities between this framework and the principles in the March 2024 OMB Memo, the AI Framework does not apply to agency acquisitions or uses of AI for non-national security systems.

The AI Framework establishes a broad set of governance practices and safeguards, categorized in four "pillars": (1) AI use restrictions, (2) minimum risk management practices for "high-impact" and "federal personnel-impacting" AI, (3) cataloguing and monitoring the use of AI, and (4) agency workforce training and accountability in the development and use of AI.

Although these pillars share similarities with the requirements of the March and October 2024 OMB Memos and the OMB's August 2024 Agency AI Reporting Guidance, the Framework also contemplates a number of novel requirements and restrictions for AI used in national security systems.

These Framework pillars collectively satisfy the AI governance and risk management requirements of § 4.2 of the AI NSM.

A. Prohibited, High-Impact, and Federal Personnel-Impacting AI Uses

Prohibited AI Use Cases. Pillar I of the AI Framework sets out a list of prohibited AI use cases that pose "unacceptable levels of risk" or that could violate "domestic or international law obligations." Specifically, agencies may not use any AI system "with the intent or purpose" to:

- Profile, target, or track individuals' exercise of legal and constitutional rights
- Unlawfully suppress or burden free speech rights or the right to an attorney
- Unlawfully disadvantage individuals based on protected categories
- Detect, measure, or infer emotional states using personal data
- Infer or determine individuals' personal characteristics based solely on biometric data
- Determine collateral damage and casualty estimations "prior to kinetic action" without rigorous testing and assurance and oversight by trained personnel
- Adjudicate or render final determinations of immigration classification, entry, or admission into the United States
- Produce and share intelligence based solely on AI outputs without notice to readers
- Remove human-in-the-loop oversight for actions "critical to informing and executing decisions by the President to initiate or terminate nuclear weapons employment"

Although some of these prohibited use cases parallel those in legislation like the pending PREPARED for AI Act (which would prohibit agencies from developing or procuring AI for emotion recognition, social scoring, inference of personal characteristics, or other uses deemed by agencies to pose unacceptable risks), as noted, the March and October 2024 OMB Memos do not contain categorical prohibitions related to non-national security uses of AI.

High-Impact AI Use Cases. In addition to outlining prohibited AI uses, Pillar I also defines certain categories of AI that may only be deployed by agencies with specific safeguards and limitations. "High-impact" AI use cases are defined by the AI Framework to "include AI whose output serves as a principal basis for a decision or action that could exacerbate or create significant risks to national security, international norms, democratic values, human rights, civil rights, civil liberties, privacy, or safety."

While agencies must evaluate each use of AI to determine whether it meets this definition, the AI Framework provides a "non-exhaustive list" of high-impact activities that, if AI is used to control or significantly influence their outcome, are "presumed to be high impact." These include the list of AI uses that are "presumed to be safety-impacting" under Appendix I of the March 2024 OMB Memo if they occur in the United States, impact U.S. persons, or affect U.S. immigration processes, entry, or admission. Other presumed high-impact AI use cases include:

- Real-time tracking or identifying individuals using biometrics for military or law enforcement action
- Classifying individuals as known or suspected terrorists, insider threats, or other national security threats to inform decisions affecting certain rights and opportunities
- Determining immigration classification or entry or admission into the United States
- Developing, testing, managing, or decommissioning sensitive chemical, biological, radiological, or nuclear materials, devices, or systems with the "risk of being unintentionally weaponizable"
- Deploying malicious software that allows AI to write code without human oversight in ways that risk "unintended performance or operation, spread autonomously, or cause physical damage to or disruption of critical infrastructure"
- Using AI as a "sole means" of producing and sharing "finished intelligence analysis"

Federal Personnel-Impacting AI Use Cases. Finally, Pillar I of the AI Framework establishes another new category of AI use cases—"federal personnel-impacting" AI—that, like high-risk AI, require agencies to implement certain safeguards prior to deployment. Federal personnel-impacting AI is defined to include "AI whose output serves as a significant basis for a decision or action resulting in a legal, material, binding, or similarly significant effect" on military service members, federal government workers, or individuals offered employment by a federal agency.

Agencies must also review each AI use case to determine if it qualifies as federal personnel-impacting. The AI Framework also lists AI uses that are "automatically presumed to impact Federal personnel" if the AI is used to control or significantly influence the outcomes of:

- Hiring decisions, including determining pay or benefits
- Decisions to promote, demote, or terminate employees
- Decisions determining job performance, physical health, or mental health diagnoses or outcomes for U.S. government personnel.

The AI Framework requires Department Heads to add new AI use cases to its lists of prohibited or "presumed" high risk or federal personnel-impacting AI uses, as needed, and to maintain unclassified public lists of AI uses deemed prohibited or high-impact.

B. Minimum Risk Management Practices and Safeguards for High-Impact and Federal Personnel-Impacting AI

Just as the March 2024 OMB Memo requires agencies to implement minimum risk management practices for safety- and rights-impacting AI in non-national security contexts, Pillar II of the AI NSM's AI Framework establishes

a "minimum baseline" of safeguards for managing risks arising from national security uses of AI that are deemed high-impact or federal personnel-impacting uses.

Minimum Risk Management Practices for High-Risk AI. Agencies must implement a large set of testing, documentation, oversight, and other safeguards prior to deploying high-impact AI. Similar to the March 2024 OMB Memo, the AI Framework requires agencies to (1) conduct "AI risk and impact assessments," including the intended purpose and expected benefit, potential risks and mitigations, and quality and appropriateness of relevant data; (2) performance testing in "realistic" contexts; and (3) independent evaluations of the intended purpose and deployment.

Additionally, agencies must identify and mitigate unlawful discrimination, harmful bias, overreliance on AI, and other emerging risks; provide appropriate training and assessments for operators; ensure human oversight of AI decisions and actions; and conduct regular monitoring, testing, and human reviews. Finally, agencies that deploy high-risk AI must maintain appropriate internal channels for reporting improper AI uses and obtaining senior-leadership approval for AI that could pose "significant degrees of risk," harm the reputation or foreign policy interests of the United States, or significantly affect "international norms of behavior."

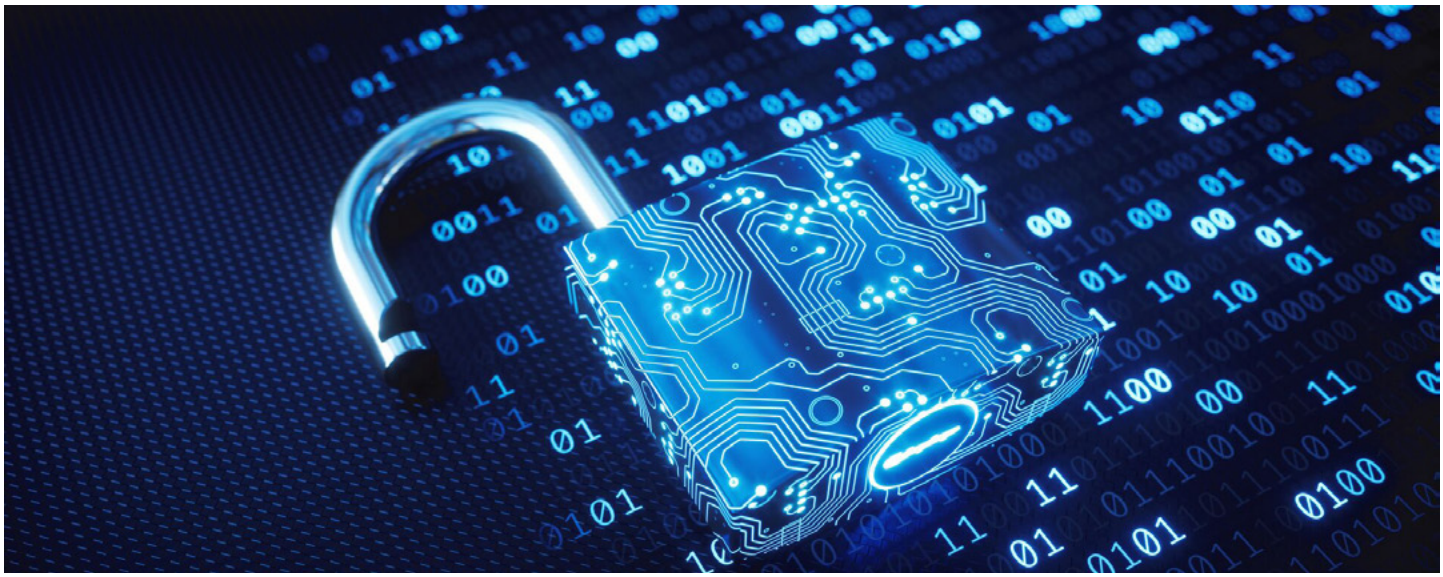
Although these minimum risk management practices are required only for high-risk AI uses, the AI Framework encourages agencies to apply these practices to all AI use cases "to the extent practicable and appropriate."

Procedural Safeguards for Federal Personnel-Impacting AI. Pillar II also requires agencies that deploy federal personnel-impacting AI to implement certain safeguards. Specifically, agencies that use AI that impact federal personnel must (1) consult and incorporate feedback from the workforce when developing and deploying federal personnel-impacting AI; (2) notify and obtain consent from affected individuals; (3) notify individuals when AI is used to inform an adverse employment-related decision or action that concerns them; and (4) provide timely human consideration and potential remedy when individuals appeal or dispute AI decisions.

C. AI Inventories, Data Management, and Oversight

The AI NSM's AI Framework establishes agency inventory and documentation requirements similar to the OMB's Agency AI Reporting Guidance. Specifically, Pillar III of the AI Framework requires agencies to conduct annual inventories of all high-impact AI use cases, which must be reported to the Assistant to the President for National Security Affairs and must include descriptions of the AI's purpose, benefits, and risks, and the agency's mitigations.

Pillar III also requires agencies to establish or update data management policies and procedures to "prioritize[e] enterprise applications and account[] for the unique attributes of AI systems," with "special consideration" for high-impact AI. Updated data management policies and procedures must address evaluations of AI training data and related risks, best practices and standards for training data and prompts, and the handling of AI models with multiple uses or trained on sensitive, inaccurate, or ill-gotten information. These data management policies must also include guidelines for using AI to make automated, mission-critical determinations and in ways that protect civil liberties, privacy, and human rights, and standards for evaluating and auditing AI.



Finally, Pillar III of the AI Framework implements certain internal agency oversight and transparency previously established by the March 2024 OMB Memo. As outlined in the March 2024 OMB Memo, agencies must appoint Chief AI Officers ("CAIOs") with necessary skills and expertise to provide advice, institute governance and oversight, and manage a host of other responsibilities related to agencies' uses of AI and compliance with the AI NSM. Agencies must also establish AI Governance Boards for reviewing and mitigating barriers to AI development and use, and must designate officials to provide oversight of agency AI activities, such as reviewing, reporting, and documenting incidents of misuse. On at least an annual basis, agencies' privacy and civil liberties officers or other oversight officials must submit reports on AI oversight activities to the head of their respective agencies, in an unclassified form "to the greatest extent practicable."

D. Agency Workforce Training and Accountability for AI

To ensure that agencies have sufficient training and expertise to carry out the functions above, agencies must establish workforce training requirements and guidelines for the responsible use and development of AI, including AI risk management training and AI training for privacy and civil liberties officers.

Such policies and procedures must be updated as needed to ensure adequate accountability. Agencies may not deploy AI systems without updated accountability policies and procedures, which must identify personnel responsible for assessing risks across the AI lifecycle, establish mechanisms for holding personnel accountable for contributions to and uses of AI decisions, require documentation and reporting, and provide channels for reporting AI misuse, investigations, and corrective actions.

4 Acquisition and Procurement of AI for National Security Purposes

A. Enabling Effective and Responsible Use of AI

To "accelerate the use of AI in service of its national security mission," § 4.1(d) of the AI NSM directs the U.S. Government to implement "coordinated and effective acquisition and procurement systems" for AI. This includes an increased capacity to "assess, define, and articulate AI-related requirements for national security purposes" and enhanced accessibility for AI companies that "lack significant prior experience working with the United States Government."

Furthermore, § 4.1(e) outlines specific actions to support these goals. DOD and the Office of the Director of National Intelligence ("ODNI"), in coordination with OMB and other relevant agencies, must establish a working group focused on procurement issues for DOD, the Intelligence Community, and national security systems. This working group may consult with the NSA Director in forming "recommendations for acquiring and procuring AI" for national security systems.

The AI NSM requires this working group to submit written recommendations to the Federal Acquisition Regulatory Council ("FARC") regarding regulatory changes to promote the following objectives related to DOD and Intelligence Community AI acquisitions.

These recommendations should promote the objectives of:

- Establishing clear standards to assess and encourage the safety, security, and reliability of AI systems;
- Streamlining the process for acquiring AI while upholding necessary safety measures;

- Simplifying contracting procedures to make it easier for companies with limited government experience to participate while simultaneously supporting a competitive AI industry;
- Designing procurement competitions that encourage broad participation and focus on technical quality to ensure the government receives optimal value;
- Enabling agencies to share AI resources where appropriate to maximize utility across government; and
- Allowing agencies with unique mandates to adopt additional policies as needed to fulfill their specific missions.

The FARC must then consider amendments to the Federal Acquisition Regulation to codify recommendations from the working group.

Additionally, DOD and ODNI are tasked with engaging, "on an ongoing basis with diverse United States private sector stakeholders," including AI technology and defense companies and the U.S. investor community, in order to understand emerging capabilities that could support or impact the national security mission.

B. Sharing and Interoperability of AI Functions on National Security Systems Across Agencies

Section 4.1(j) emphasizes the need for better internal coordination across the U.S Government regarding AI use in national security systems to facilitate interoperability, resource sharing, and economies of scale offered by advanced AI models.

In turn, § 4.1(k) outlines actions to achieve these goals. DOD and ODNI must regularly issue or update guidance to improve the consolidation and interoperability of AI-related functions across national security systems in order to ensure effective coordination and resource sharing where permitted by law. This guidance must focus on:

- Recommending organizational practices that enhance AI research and deployment across multiple national security entities to create consistency in these practices wherever possible;
- Facilitating centralized efforts in research, development, and procurement of general-purpose AI tools and infrastructure to enable shared access among agencies, while safeguarding sensitive information as needed;
- Standardizing AI-related national security policies agencies where appropriate and legally permissible; and
- Establishing protocols for sharing information between DOD and the Intelligence Community when contractor-developed AI systems present risks to safety, security, trustworthiness, or raise concerns about human rights, civil rights, civil liberties, or privacy.

C. Agency Guidance on AI Governance and Risk Management for National Security Systems

Section 4.2(g) provides agency guidance of AI governance and risk management for national security systems. The heads of the Department of State, Treasury, Commerce, DOD, the Department of Justice ("DOJ"), DOE, DHS, ODNI, and other agencies using AI in national security systems must issue or update guidance for AI governance and risk management aligned with the policies in the AI NSM, the AI Framework discussed above, and other applicable policies. Agencies must review and revise this guidance annually, which should remain unclassified and available to the public, as appropriate, with an option for a classified annex if needed. APNSA must, in turn, organize an annual interagency meeting to promote consistency in AI governance and risk management across agencies, while respecting each agency's unique roles and responsibilities.

Areas that APNSA must target for alignment include:

- Risk management practices for high impact AI;
- Standards and activities for AI and AI systems, including training, testing, accreditation, security, and cybersecurity; and
- Additional matters impacting interoperability of AI and AI systems across agencies.

5 Additional Provisions

The AI NSM addresses a wide range of issues and priorities relevant to the use of AI to advance U.S. national security. In addition to the assessment, risk management, and procurement frameworks discussed above, the AI NSM directs agencies to make progress on a number of government priorities for AI, including attracting and retaining AI talent, promoting and protecting assets critical for AI infrastructure, and collaborating with U.S. allies on AI, while protecting U.S. AI-related assets from foreign adversaries.

Attracting and Retaining AI Talent in Government

Section 3.1(c) of the AI NSM requires APNSA to convene relevant agencies to "explore actions for prioritizing and streamlining administrative processing operations for all visa applicants working with sensitive technologies." Relatedly, § 4.1(c) directs the Intelligence Community elements and the Departments of State, Defense, Energy, Justice, and Homeland Security to review their hiring and retention policies and strategies to accelerate AI adoption, education, and training.

Promoting AI Semiconductors and Computational Infrastructure

Recognizing that the "current paradigm of AI development depends heavily on computation resources" like AI semiconductors and AI-dedicated computational infrastructure, § 3.1(e) instructs the National Science Foundation to use the National AI Research Resource (NAIRR) pilot, established by the 2023 AI Executive Order, to "distribute . . . critical assets for AI development to a diverse array of actors that otherwise would lack access to such capabilities." The White House Chief of Staff must also coordinate efforts to "streamline permitting, approvals, and incentives for the construction of AI-enabling infrastructure, as well as surrounding assets supporting the resilient operation of this infrastructure."

Protecting U.S. AI from Foreign Intelligence Threats

In response to foreign state efforts to "obtain and repurpose the fruits of AI innovation in the United States to serve their national security goals," including through the use of "gray-zone methods" to obtain U.S. AI-related intellectual property (referred to as "critical technical artifacts"), § 3.2 of the AI NSM directs ODNI to identify critical nodes and plausible risks of disruption or compromise in the AI supply chain. This section also requires CFIUS to consider whether covered transactions involve foreign access to proprietary information on AI training techniques and other proprietary insights on the creation and use of powerful AI systems.

Rapid Development and National Security Use of AI.

In addition to mitigating risks, the AI NSM aims to accelerate effective national security uses of AI. Section 4.1(g) directs DOD and the Intelligence Community to review and revise policies and procedures to enable the effective use of AI, accounting for use of personal information or IP in datasets, risks of algorithmic bias or other AI failure modes, and other issues. These agencies must also consider future "guidance that shall be developed by DOJ, in consultation with DOD and ODNI, regarding constitutional considerations raised by the IC's acquisition and use of AI." These changes must be consistent with national security system policies and OMB guidance governing AI security on non-national security systems.

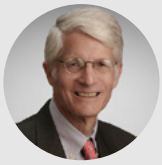
Co-Development and Co-Deployment of AI with Allies and Partners.

To invest in and enable "co-development and co-deployment of AI capabilities with select allies and partners," § 4.1(i) directs DOD to evaluate the feasibility of advancing the co-development and shared use of AI and AI-enabled assets with select allies and partners, including a list of foreign states for potential co-development or co-deployment and a list of bilateral and multilateral fora for outreach.

Ryan Burnette
Government Contracts / Data Privacy and Cybersecurity Special Counsel, Washington
+1 202 662 5746
RBurnette@cov.com

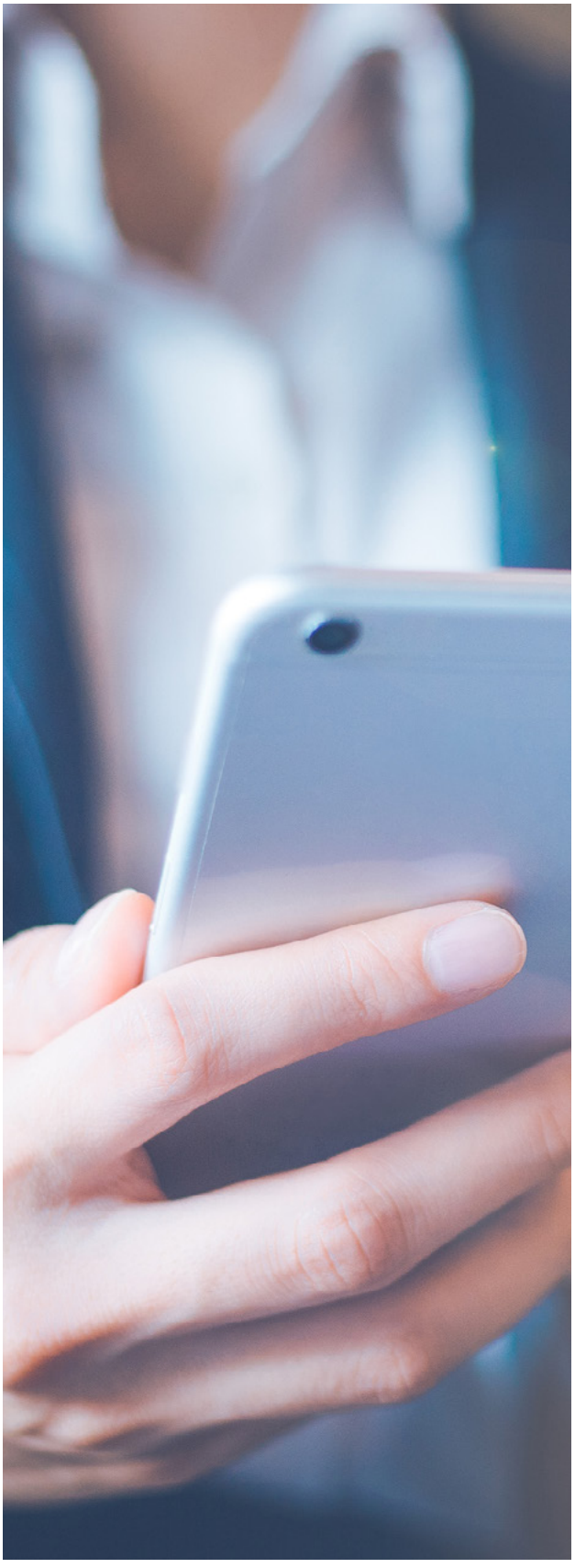
Nooree Lee
Government Contracts Partner, Washington
+1 202 662 5909
NLee@cov.com

August Gweon
Data Privacy & Cybersecurity Associate, Washington
+1 202 662 5149
AGweon@cov.com



Robert Huffman
Government Contracts Senior Of Counsel, Washington
+1 202 662 5645
RHuffman@cov.com

Likely Trends in U.S. Tech and Media Regulation Under the New Trump Administration



With U.S. President Trump returning to the White House, we expect the regulatory landscape facing technology and communications companies to shift significantly, if not uniformly. On the one hand, media and telecommunications companies that have long been regulated heavily by the FCC can likely expect a more deregulatory environment than they have experienced under the Biden Administration (with potential caveats). On the other, large technology companies, which have largely avoided heavy-handed regulation, can expect to face a more active regulatory environment aimed at limiting or preventing content moderation decisions that the incoming Administration has characterized as "censorship" of conservative viewpoints. Meanwhile, bipartisan priorities—such as the commitment to ensuring national security in the telecommunications sector—will likely continue to be a major focus of regulatory agencies. While the assessments of regulatory risks and opportunities will continue to be refined and updated as the next Trump administration takes shape, we highlight here a few trends that are likely to influence policy and regulation at the FCC over the next four years.

Changes in Regulation: Deregulation for Some, Greater Scrutiny for Others

FCC Commissioner Brendan Carr, who is the frontrunner to be named the next Chair of the FCC, has a long history of public statements supporting deregulation of the industries historically regulated by the FCC. For instance, Carr has observed in the past that "rapidly evolving market conditions counsel in favor of eliminating many of the heavy-handed FCC regulations that were adopted in an era when every technology operated in a silo." This

likely means that we can expect to see a Republican-led FCC seeking opportunities to loosen regulations on broadcasters, the pay TV industry, and internet service providers, ranging the gamut from reform of broadcast licensee ownership restrictions to repealing (or supporting the court reversal of) the Biden-era net neutrality order.

However, other industries under the FCC's umbrella may face greater scrutiny. In particular, we anticipate that the FCC's interest in national security policymaking will continue to grow, as Commissioner Carr has highlighted issues such as curbing the influence of foreign nations on social media platforms and expanding the FCC's list of providers of communications equipment and services that pose an unacceptable risk to the national security of the U.S. This interest could expand beyond traditional telecommunications providers to other technology enterprises, such as those that offer high-powered cloud computing services to customers in China and elsewhere.

Different Approach to Transaction Reviews

With the strong economic headwinds facing traditional, linear media, we expect a Republican-led FCC will be more open to consolidation as a strategy for growth, if not survival. This openness may materialize through the Commission's quadrennial review of its media ownership rules, or through standalone rulemakings, such as the still-pending proceeding from the last Trump administration considering whether the FCC should revise the national ownership cap for broadcast television and the UHF discount. As a result, we also expect that the FCC will be more receptive to a broader range of media transactions than in the recent past. Looking beyond the media sector, it is possible that this openness could extend to wireless and satellite communications companies, reflecting the rapidly shifting dynamics in the communications market as information and entertainment is delivered to consumers in new ways.

Pressure on Tech Companies to Play a More 'Neutral' Role in Public Debates

Both President-elect Trump and Commissioner Carr have been vocal in support of government action to reign in perceived abuses by large technology companies. In a video about President Trump's "plan to shatter the left wing censorship regime" originally posted in 2022 but recently reshared by Elon Musk on X (f/k/a Twitter) and Robert F. Kennedy Jr. on YouTube, the President-elect said that he would ask the Congress to enact reforms to Section 230 and adopt a Digital Bill of Rights, among other actions aimed at prohibiting and/or mandating certain content moderation policies by the largest technology companies. For example, President-elect Trump said that "all users over the age of 18 should have the right to opt out of content moderation and curation entirely and receive an unmanipulated stream of information if they so choose."

Commissioner Carr has expressed support for specific policies along these lines that would reduce the scope of immunity granted by the Section 230 safe harbor and increase transparency into search and content moderation decisions. In short, the incoming Administration very likely will continue to put pressure on technology companies to play less of a role in content moderation, in tension with trends in other regions (including Europe and Brazil, for example) and some state-level trends. This means that technology companies will have to navigate these federal policies against competing policy objectives originating from "blue" states like California and regulators in Europe and elsewhere.

One area where administration policy may ultimately align with European regulatory pressures could be on reforms to the Universal Service Fund (USF). Republican policymakers, including Commissioner Carr, have long argued that the large tech platforms—such as social media platforms, search engines, and streaming services—have been "free-riders" with regard to the funding mechanisms for major telecom programs through the USF. And as the pool of eligible contributors to the USF continues to shrink, practical pressures will ultimately require changes to the existing funding mechanism. We expect that a Republican Congress and FCC will actively explore measures to require these platforms to make contributions to support these programs directly.

SEC Enforcement Sweep Reaffirms Focus on Anti-Whistleblower Provisions in Employee Agreements

On September 9, 2024, the SEC announced settled enforcement actions against seven companies for violating the SEC's whistleblower rules.[1] Specifically, the SEC alleged that the companies had provisions in various kinds of agreements with employees, including employment, separation, and settlement agreements, that purport to restrict, and thereby could potentially discourage, employees and other signatories from reporting information to government investigators or participating in a whistleblower award.

The Dodd-Frank Act of 2010 gave the SEC authority to administer and enforce a whistleblower program. Among the rules the SEC has adopted to implement that authority is Exchange Act Rule 21F-17(a)[2]:

> **No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement (other than [certain specified] agreements ... related to the legal representation of a client) with respect to such communications.**

The recent actions are not the first the SEC has brought under this provision.[3]

The SEC often collects related cases into a "sweep" to heighten attention and amplify its message. In the recent seven actions, the agreements include employment, severance, retention, separation, consulting, and settlement agreements that stretch over the last five years. The contracts included clauses that waived the right to a monetary award in any government investigation, waived the right to file a complaint or claim with a government authority, and required prior notification before sharing confidential information with a governmental authority. The SEC was not, apparently, moved by clauses that limited these restrictions "to the fullest extent permitted by law."

In its sweep, the SEC included companies from various industries, including fashion, healthcare, software, manufacturing, and consumer credit reporting. (It is not clear how the companies were identified.) Penalties ranged from $19,500 (against a company with a going concern opinion and $8,890 in cash) to $1,386,000. The amounts are not explained, but seem to bear some relation to the number of contracts with which the SEC took issue. The SEC assessed penalties notwithstanding the companies' remedial efforts once approached by the SEC and the fact that the provisions had never been invoked to prevent a party from making a claim or seeking compensation as a whistleblower.

The SEC's message could not be clearer – if public companies have any contractual provisions that restrict the ability to report potentially wrongful conduct to the SEC and participate in a whistleblower award, the SEC is likely to object and may take action against such companies. The financial and reputational consequences to the company can be significant. Public companies should review their standard agreements with employees to determine whether they contain similar, potentially problematic, provisions, and make any necessary updates. The SEC stresses that its investigation in this area is ongoing.

Lindsay Burke
Employment
Partner, Washington
+1 202 662 5859
LBurke@cov.com

Matthew Franker
Capital Markets and Securities
Partner, Washington
+1 202 662 5895
MFranker@cov.com

David Fredrickson
Capital Markets and Securities
Senior of Counsel, Washington
+1 202 662 5083
DFredrickson@cov.com

Gerald Hodgkins
Securities Litigation and Enforcement
Partner, Washington
+1 202 662 5263
GHodgkins@cov.com

New HSR Requirements are set to become effective from February 10, 2025

Significant changes to the U.S. merger notification regime under the Hart-Scott-Rodino ("HSR") Act are slated to become effective from February 10, 2025, based on an update to the Federal Register publication on November 12, 2024.

All HSR filings made on or after February 10, 2025, will be required to conform to the new rules; filings made prior to that date must be made according to the current rules.

The Final Rule, which scaled back the scope of the changes initially proposed in June 2023, is still expected to add significant increased burden to filing parties.

We monitor these issues closely and stand ready to assist companies in navigating these transitions. We will continue to issue alerts in light of further developments.

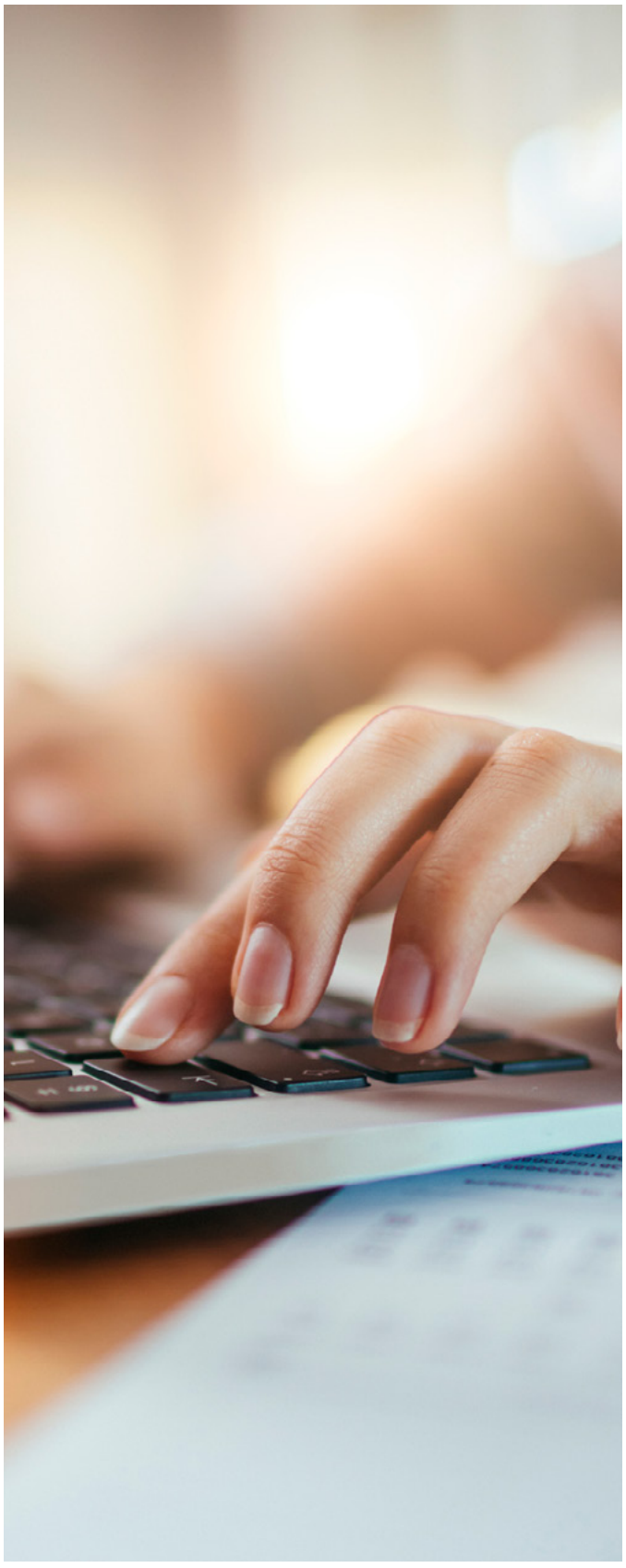
Thomas O'Barnett
Antitrust/Competition
Partner, Washington
+1 202 662 5407
TBarnett@cov.com

James O'Connell
Antitrust/Competition
Partner, Washington
+1 202 662 5991
JOConnell@cov.com

Anne Lee
Antitrust/Competition
Partner, Washington
+1 202 662 5535
ALee@cov.com

Ryan Quillian
Antitrust/Competition
Partner, Washington
+1 202 662 5329
RQuillian@cov.com

Five key takeaways from recent EU developments on the GDPR's "legitimate interests" legal basis



There have been significant developments relating to the "legitimate interests" legal basis under Article 6(1)(f) of the GDPR:

- On 4 October 2024, the Court of Justice of the EU ("CJEU") handed down its judgment in a case relating to the Royal Dutch Lawn Tennis Association (Case C-621/22, KNLTB), confirming that "commercial" interests when processing personal data can constitute legitimate interests.
- On 8 October 2024, the European Data Protection Board ("EDPB") adopted its long-awaited draft guidelines on when controllers can rely on legitimate interests ("Draft Guidelines"), which update a 2014 opinion from the Article 29 Working Party ("WP29"). Consultation on the Draft Guidelines closed on 20 November 2024

We set out below five key takeaways from the Draft Guidelines and the KNLTB case, and how these developments may affect a GDPR-regulated data controller's ability to rely on legitimate interests in the future to process personal data.

I. Commercial interests can be a "legitimate" interest

The CJEU has consistently held that relying on the legitimate interests legal basis requires controllers to pass a three-step test. The first limb of the test requires controllers to establish that their processing supports "legitimate interests" pursued by the controller or a third party. In the *KNLTB* case, the Dutch data protection supervisory authority ("SA") asked the CJEU questions about the nature of those interests: specifically, whether commercial interests could be legitimate.

The background here seemed relatively innocuous: could the tennis club, a data controller, rely on legitimate interests to share data about its members with third parties for marketing purposes? The Dutch SA concluded that it could not, and that it failed the first limb of the test because the interests pursued by its processing were "commercial" and any interest, in order to be "legitimate", must be determined by or reflected in law. The SA imposed a fine of 525,000 Euros upon the tennis club for the GDPR breach. It

appealed, and a Dutch court asked the CJEU to clarify whether a controller can, in principle, rely on: (a) legitimate interests that are not expressly identified in law; and (b) on "commercial" interests. In a relatively short judgment, the CJEU confirmed that controllers can rely on legitimate interests not affirmatively or positively established in law, and that commercial interests can, in principle, constitute legitimate interests provided that those commercial interests are not unlawful. This is a welcome ruling for controllers, who will be able to continue to take the position that they can rely on legitimate interests for various commercial practices, provided that they also meet the second and third limbs of the assessment.

The Draft Guidelines reiterate this position, but also note that to be "legitimate," the interests pursued must be clearly and precisely articulated, and real and present.

This suggests: (a) that there are close links between relying on legitimate interests and the GDPR's transparency obligations (under which controllers must identify the legitimate interests they pursue); and (b) that hypothetical interests will not be sufficient.

II. Controllers have to consider carefully whether processing is "necessary" to meet each of the interests they pursue

In the Draft Guidelines, the EDPB reiterates the CJEU's prior holdings in relation to the second limb of the legitimate interests test: that processing will be necessary to meet legitimate interests only where there are no "reasonable, just as effective, but less intrusive alternatives."

Notably, however, the Draft Guidelines state that "in practice, it is generally easier for a controller to demonstrate the necessity of the processing to pursue its own legitimate interests than to pursue the interests of a third party."

To the extent that controllers rely on third parties' interests when they use the legitimate interests legal basis, they are likely to have to consider this necessity requirement particularly carefully.

III. The EDPB's assessment of the third limb of the balancing test appears to make it more challenging to rely on legitimate interests than the WP29's 2014 opinion

The third limb of the legitimate interests test requires controllers to balance the interests they pursue against the rights, freedoms, and interests of affected data subjects. The EDPB's Draft Guidelines emphasize, again consistent with CJEU jurisprudence, that this requires a case-by-case assessment taking into account a number of factors, including the impact of the processing on affected data subjects, their reasonable expectations, and the safeguards the controller has put in place. The way that the Draft Guidelines structure the balancing assessment, however, suggests that there is a higher bar for relying on legitimate interests than was set out in the WP29's pre-GDPR opinion. For example:

- Unlike the 2014 opinion, the EDPB does not expressly state that the strength of the legitimate interests pursued by a controller is a relevant factor in the balancing test;
- The EDPB also expressly states that measures a controller has taken to comply with the GDPR are not relevant, even though those measures (e.g., transparency, the right to object, short retention periods, and security measures) could clearly mitigate the impacts of the processing on data subjects; and
- The Draft Guidelines indicate that transparency measures will not necessarily assist a controller in setting a data subject's reasonable expectations, and that simply because processing is common practice does not mean that it would be within their reasonable expectations.

We expect that some stakeholders might raise concerns about some of these points in the consultation.

IV. The EDPB reiterates the high bar that exists for establishing compelling legitimate grounds and rejecting objections to processing under Article 21 GDPR

Article 21(1) grants data subjects the right to object to any processing carried out on the basis of legitimate interests "on grounds relating to [their] particular situation," and that the controller must cease the processing unless they have "compelling legitimate grounds" that override the data subject's rights, freedoms, and interests. The Draft Guidelines set out the EDPB's view that a high bar must be met when rejecting an objection. It states that:

- Even if a data subject does not elaborate much on their particular situation in any detail, that is not per se a reason to reject an objection (if the controller has doubts as to the "particular situation" of the data subject, it can ask them to elaborate); and
- When conducting the balancing test following an objection, the controller may only take into account "compelling" legitimate interests, and not all legitimate interests will meet this standard. The interests must be "essential" to the controller—for example if the processing is necessary to protect the controller or systems from "serious immediate harm or from a severe penalty which would seriously affect its business."

V. The EDPB indicates that it is possible to rely on legitimate interests to share data with public authorities (in the EU)

In the 2023 *Meta v Bundeskartellamt* case (C-252/21), the Court was asked whether Meta could collect data on an ongoing basis from other group services as well as from third-party websites and apps for the purpose of sharing information with law-enforcement agencies and responding to legal requests in order to prevent, detect and prosecute criminal offences, unlawful use, breaches of the terms of service and policies, and other harmful behaviour.

In response, the Court stated that "the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences . . . is not capable, in principle, of constituting a legitimate interest pursued by the controller" because in relation to a private entity, that processing "is unrelated to its economic and commercial activity." This holding, viewed in isolation, understandably has caused some alarm.

The Draft Guidelines attempt to provide more clarity based on the GDPR and the ruling in Meta. In particular, the EDPB states that a private entity can rely on legitimate interests to "report to law enforcement authorities possible criminal acts or threats it may occasionally become aware of." The Draft Guidelines contrast this with "collect[ing] and stor[ing] personal data in a preventive ***and systematic manner*** specifically to be able to provide such data to law enforcement authorities" (our emphasis).

The Draft Guidelines also provide that a controller could, in some scenarios, have a legitimate interest in disclosing personal data in response to requests from a third country (i.e., non-EU/EEA) law enforcement authority or public administration, "in particular if the controller is subject to third country legislation and non-compliance with such request would entail sanctions under foreign law". This analysis is context-dependent. The EDPB reiterates that it has in the past, based on a specific set of facts, taken the view that the interests or fundamental rights and freedoms of the data subject overrode the controller's interest in complying with a request from a third country law enforcement authority to avoid sanctions for non-compliance.

Dan Cooper
Data Privacy and Cybersecurity
Partner, Brussels
+32 2 545 7527
DCooper@cov.com

Mark Young
Data Privacy and Cybersecurity
Partner, London
+44 20 7067 2101
MYoung@cov.com

Paul Maynard
Data Privacy and Cybersecurity
Special Counsel, London
+44 20 7067 2381
PMaynard@cov.com

Tomos Griffiths
Data Privacy and Cybersecurity
Associate, London
+44 20 7067 2178
TGriffiths@cov.com

ECJ decides that EU Member States cannot refer below-threshold transactions to the European Commission (Illumina/Grail v Commission)

On 3 September 2024, the European Court of Justice ("ECJ") published its highly-anticipated judgment in *Illumina/Grail v Commission* (Joined Cases C 611/22 P and C 625/22 P) ("ECJ Judgment"), regarding the scope of application of Article 22 of the EU Merger Regulation ("EUMR").

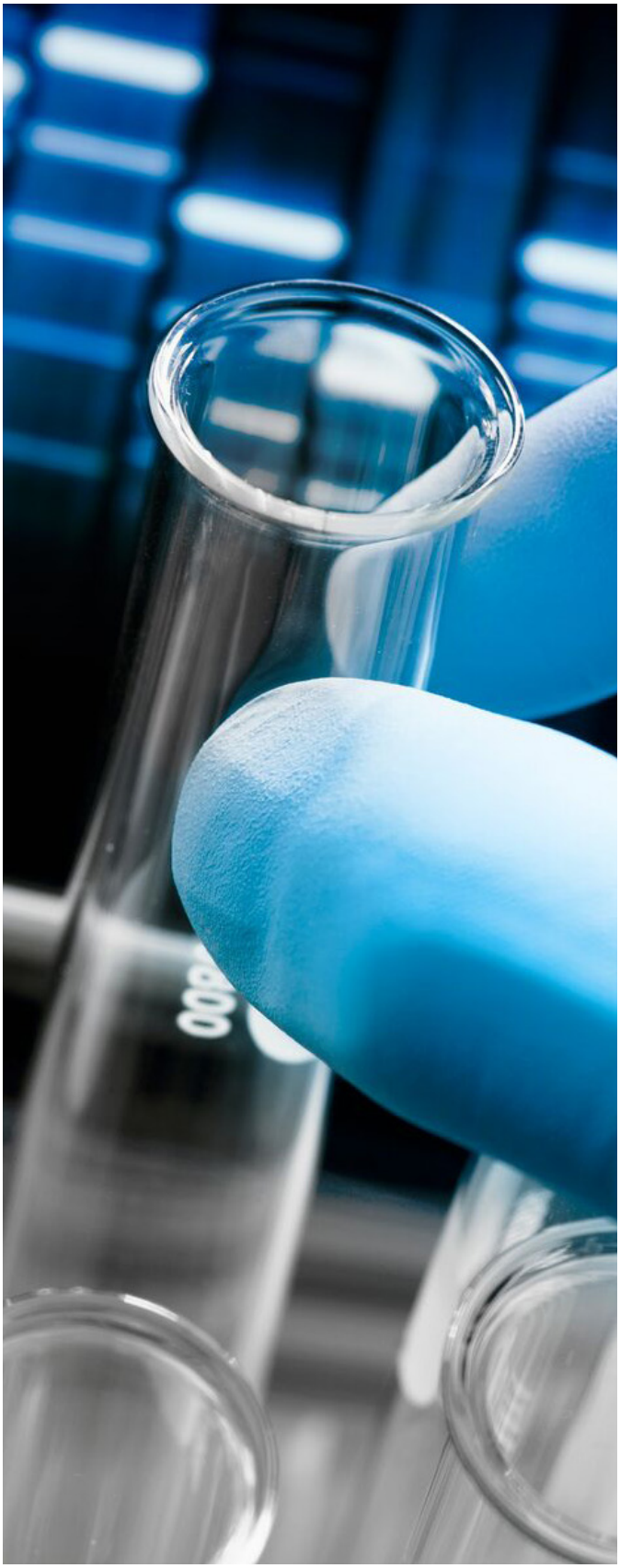
The ECJ set aside the EU General Court ("GC") judgment (Case T 227/21) and ruled that the European Commission ("Commission") does not have jurisdiction over transactions referred to it by the national competition authorities of EU Member States ("NCAs") if the transactions do not meet the national thresholds of the referring EU Member States.

Background to the case

On 20 September 2020, Illumina Inc. ("Illumina"), a US-based gene-sequencing company, agreed to acquire Grail LLC ("Grail") (together, the "Parties") which develops blood tests for the early detection of cancer (the "Acquisition"). Since Grail had no revenue in the EU, the Acquisition triggered neither the EU nor the EU Member State merger control thresholds; therefore, it was not notified to the Commission or any NCA.

However, following a complaint, the Commission invited the NCAs to submit a request under Article 22 EUMR for the Commission to review the Acquisition ("Referral Request"). In response, the French NCA submitted this Referral Request, and the Belgian, Greek, Icelandic, Dutch and Norwegian NCAs asked to join. Simultaneously announcing its shift from prior policy, the Commission took the view that Article 22 EUMR allows NCAs to refer to it for review transactions which fall below the referring EU Member States' national thresholds (i.e., where the referring NCAs do not have jurisdiction themselves) if they (i) amount to an EUMR 'concentration'; (ii) affect trade between EU Member States; and (iii) threaten to significantly affect competition in the requesting EU Member State(s).

Accepting the Referral Request, the Commission ordered Illumina to notify the Acquisition. The Commission eventually prohibited the transaction and fined the Parties for violating the EU standstill prohibition (or 'gun jumping') since they had closed the transaction during the Commission's in-depth investigation.



In addition to separate appeals – relating to the interim hold-separate orders, the gun jumping fine, and the eventual prohibition by the Commission of the Acquisition – the Parties appealed to the GC, arguing that the Commission does not have jurisdiction over transactions in response to referral requests from NCAs that do not themselves have jurisdiction. The GC rejected the appeal: according to a literal, historical, contextual, and teleological interpretation of Article 22 EUMR and the EUMR itself, the GC found that NCAs could ask the Commission to examine transactions which fall below their national thresholds.

Illumina and the Commission appealed to the ECJ.

The ECJ Judgment

The ECJ ruled in favour of the Parties and set aside the GC judgment. While it agreed with the GC that a literal interpretation of Article 22 EUMR suggests that "any" transaction which meets the above-mentioned conditions can be referred, this is not the case under a historical, contextual or teleological interpretation.

The ECJ held that the GC had erred in its historical and contextual interpretation of Article 22 EUMR, which instead pursues only two primary objectives: (i) at the time it was implemented, it was to permit the review of transactions that could distort competition in EU Member States which did not yet have merger control rules (at the time called the 'Dutch clause'); and (ii) it was to extend the 'one-stop shop' principle enabling the Commission to review transactions which had been notified in several EU Member States, to avoid multiple parallel reviews and thereby enhance legal certainty for companies. The ECJ further held that the GC had erred in its teleological interpretation when holding that Article 22 EUMR is a 'corrective mechanism' intended to remedy deficiencies in the merger control system. According to the ECJ, this corrective function rather concerns the allocation of competences between the Commission and NCAs, and is to limit the possibility of multiple parallel notifications, providing legal certainty and facilitating the one-stop shop principle.

The ECJ concluded that it could not be established that the Article 22 EUMR mechanism *"was intended to remedy deficiencies in the control system inherent in a scheme based principally on turnover thresholds, which is, by definition,*

Key takeaways

- Based on a historical, contextual, and teleological interpretation of Article 22 EUMR and the EUMR itself, NCAs cannot ask the Commission to examine transactions which do not meet their national thresholds.
- Article 22 EUMR provides for a corrective function regarding the allocation of competences between the Commission and NCAs, and is to limit the possibility of multiple parallel notifications, providing legal certainty and facilitating the one-stop shop principle.
- An amendment of the EUMR thresholds and/or referral rules to capture below-threshold transactions would likely entail a burdensome legislative process and complex negotiations with EU Member States.
- The Commission can still rely on (i) new thresholds which have by now been introduced in some EU Member States to catch transactions outside the scope of their traditional turnover-based thresholds, and (ii) the possibility for NCAs to review these transactions by means of Article 102 TFEU, which prohibits abuses of a dominant position.

Thanks to its long-standing expertise in merger control and its strong network of local counsel, Covington can assist clients not only in submitting all the necessary filings, but also in evaluating the risks connected to transactions falling below both the EU thresholds and traditional turnover-based national ones, and in identifying the most suitable strategy to implement the transaction with the highest degree of legal certainty.

incapable of covering all potentially problematic concentrations". Such an interpretation would be liable to upset the balance between the various objectives of the EUMR, in particular *"the effectiveness, predictability and legal certainty that must be guaranteed to the parties to a concentration".*

The need to permit effective control of all transactions could not lead to the scope of the EUMR being extended.

Likely implications of the ECJ Judgment

The Commission will likely go back to the drawing board and carefully consider its options following the ECJ Judgment. It remains a Commission policy priority to have the proper means to review certain transactions that meet neither the EU nor any EU Member State thresholds, but which may nonetheless be harmful to competition in the EU (e.g., so-called 'killer acquisitions' in which the target is a start-up with significant competitive potential that has yet to generate significant revenues).

The ***natural but long-term solution*** (suggested also in the ECJ Judgment) would be for the Commission to initiate a legislative proposal to amend the EUMR thresholds and/or referral rules, e.g., to introduce a 'call-in' mechanism for transactions that meet neither the EU nor the EU Member State thresholds.

However, such a solution would need to undergo a burdensome legislative process and complex negotiations with EU Member States whose approval would be required. In particular, opening the door for revisions to the EUMR would give EU governments the opportunity to suggest other changes to merger policy and rekindle historically controversial debates, e.g., on the treatment of national industrial "champions" of EU member states.

In the meantime, as a ***short/mid-term solution***, the Commission will likely rely on two alternative routes for reviewing certain below-threshold transactions:

- First, as confirmed in a statement from Commission Executive Vice-President Vestager in reaction to the ECJ Judgment, certain transactions could be reviewed (and referred) under new thresholds which have by now been introduced in some EU Member States to catch transactions outside the scope of their traditional turnover-based thresholds. This is the case in Italy, for example, where the Italian NCA has the power to call in transactions if (i) they meet only one of the two turnover-based thresholds (or where the total worldwide turnover of the parties exceeds EUR 5 billion) and (ii) there are real risks for competition in the national market or in a substantial part of it. Similarly in Germany, a recently-introduced 'transaction value' threshold can be triggered in cases where only the acquirer has registered global and German revenues if (ii) the transaction value (i.e., generally the consideration for the deal) exceeds EUR 400 million, and (ii) the target has 'substantial operations' in Germany – which can be indicated by revenues or assets but also by other sector-specific indicators (e.g., monthly active users in the context of certain online services). Additional EU Member States may also adopt similar rules and the Commission might encourage them to do so, to fill the perceived gap which, for now, will persist following the ECJ Judgment.
- Second, as noted in the ECJ Judgment as well, based on the *Towercast* case there is also the possibility for NCAs to conduct an ex post review of certain transactions falling below both the EU and national merger control thresholds under Article 102 TFEU, which prohibits abuses of a dominant position. However, this route remains subject to several uncertainties in terms of its practical application, e.g., regarding the competent competition authorities and the legal standard for determining when an acquisition may amount to an abuse of dominance.

That said – even if companies will need to stay attentive to EU Member State thresholds which are not based on revenue (and which can confer a certain degree of discretion on NCAs, like in Italy), and may continue to face a certain degree of uncertainty regarding the potential application of Article 102 TFEU to transactions – for now, the scope for Commission review of below-threshold transactions has been limited by the ECJ Judgment.

At the same time, the EU enforcement community (and companies) may also be looking to reactions just outside the EU: the ECJ Judgment may well increase expectations (and add more strain) on the UK Competition and Markets Authority to take the role of "global guardian" over these below-threshold transactions.

Johan Ysewyn
Antitrust / Competition
Partner, Brussels
+32 2 549 52 54
JYsewyn@cov.com

Rolf Ali
Antitrust / Competition
Associate, Brussels
+32 2 545 7507
RAli@cov.com

Alessandro Cogoni
Antitrust / Competition
Associate, Brussels
+32 2 549 5280
ACogoni@cov.com

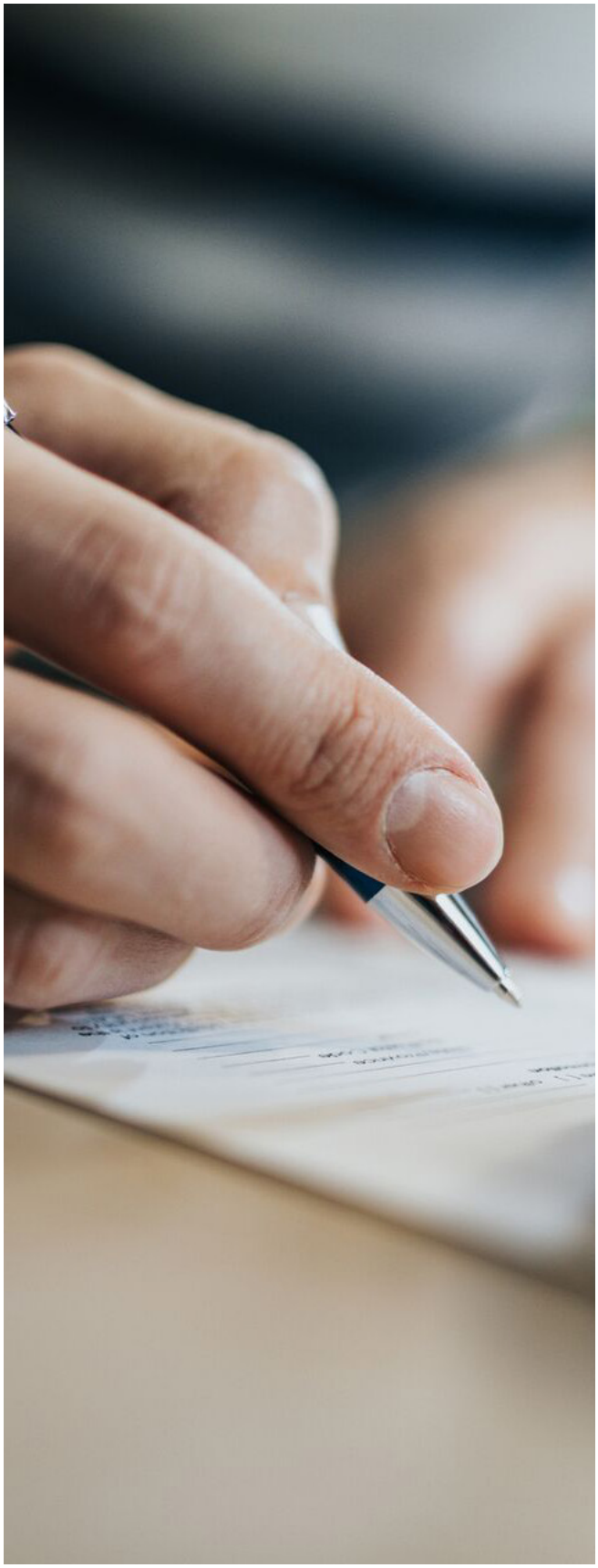
Non-Compete Clauses in the UK and U.S.- Recent Trends

What is happening?

In the U.S. and UK, the use of post-termination non-competes has recently been under scrutiny, and how effective these will be as a tool for protecting a prior employer's business in the future is unclear.

On 23 April 2024, the U.S. Federal Trade Commission ("FTC") voted to issue a final rule adopting a "comprehensive ban on new [post-termination] non-competes with all workers". The FTC's rationale for banning post-termination non-compete clauses in employment contracts is that, in its view, they constitute "unfair methods of competition", and that their cumulative effect is to suppress wages and stifle innovation. Others believe that non-competes often serve legitimate interests of businesses, such as protecting against misappropriation of their intellectual property and confidential business information, and that the FTC has not collected information sufficient to support the proposed ban. Thus, numerous legal challenges have been filed contesting the ban. The latest development is that, on August 20, 2024, a ruling by the United States District Court for the Northern District of Texas prohibits the FTC from enforcing the proposed non-compete rule nationwide, on the basis that the FTC does not have substantive competition-related rulemaking authority and the rule was arbitrary and capricious. The FTC will very likely appeal this decision (see our recent alert for more in this regard).

In spite of the challenges its proposed rule is facing, the FTC's crackdown echoes the proposed reforms to post-termination non-competes made by the UK's (former) Government in 2023. On 12 May 2023, the Conservative government announced its intention to introduce a statutory cap on post-termination non-compete clauses of three (3) months for employment and worker contracts. This would have a significant impact on market practices, given that 12 month non-competes for senior employees are relatively common. It is not yet clear when, or indeed if, the statutory cap will come into force, particularly now that the Labour Party is in power and little has been said in this regard. However, given the widespread appetite for curtailing non-competes, it seems unlikely that the new Government will take a more lenient approach and so the future effectiveness of non-competes in the UK is still uncertain.



In the vast majority of European jurisdictions, the enforcement of post-termination restrictions has always been challenging, particularly where the employee is not compensated in any way for complying with the obligation(s) following termination. For example, in Germany, a post-termination non-compete clause is invalid if there is no corresponding compensation for the employee having entered into it. Similar notions exist under French and Italian law. In contrast to the U.S. and the UK, there have not been any similar efforts in the EU to further restrict the use of post-termination non-competes in the employment context. That being said, in the antitrust context, the EU Commission seems to be paying particular attention to limiting the effectiveness of so-called non-solicitation agreements.

Why does it matter?

Post-termination non-compete clauses are commonly used in employment agreements for senior or business-critical employees, particularly in the U.S. and the UK. Businesses use them, for example, to prevent such individuals from misappropriating the intellectual property or confidential information of the business by prohibiting them from working for competitors for a limited period of time after their employment ends. Non-competes are particularly important for senior employees, but in practice workers of all levels of experience can be subject to them. In the U.S., approximately 30 million workers have non-compete clauses in their employment contracts [1]. In the UK, this figure stands at around 30% of employees [2].

Given their relative ubiquity in the U.S. and UK, the undermining (or outright ban) of non-competes would force many employers to look for different ways to protect their legitimate business interests.

In addition, these developments are likely to result in a spike in litigation between employers and departing employees. Many businesses may find themselves, for example, seeking to obtain injunctions against ex-employees from divulging important know-how to competitors and may find themselves increasingly reliant on enforcing confidentiality and intellectual property provisions, among other things. It is not clear that such measures would be as effective in protecting the legitimate business interests of employers.

What should you do about it?

Employers who operate in these markets and rely on non-competes should monitor developments in this area and perhaps consider alternative ways of effectively protecting their business interests.

In the U.S. – in spite of the challenges that the FTC's proposed rule is facing – employers should take stock of their use of non-competes, including in current employment agreements, severance agreements, consulting agreements, IP assignment agreements, confidentiality agreements, employee handbooks, and equity award agreements, as well as in any past agreements where any such non-compete provisions are still effective. Employers that have an existing practice of including non-compete clauses in arrangements with workers, or are considering doing so for the first time, should consult antitrust and employment / executive compensation counsel. If the FTC successfully appeals the recent order prohibiting its proposed rule, employers will need to determine which of their workers are subject to non-compete clauses and whether – and by when – they are required to provide notice of non-enforcement to those workers or to take other required actions.

In the UK, employers should be cautious about imposing non-competes with a long duration. Their necessity should be considered on a case-by-case basis. Whether or not the previous UK government's proposals materialize into law any time soon, courts will likely be sensitive to the policy reasons for curtailing the power of non-competes, meaning that the enforceability of longer restrictions could become more difficult to defend.

As alternatives to non-competes, employers may wish to lean more heavily on garden leave arrangements where this is possible. However, extending employees' periods of garden leave so that they effectively operate as non-competes will likely prove expensive (due, in part, to the adverse tax consequences of keeping inactive employees on the books for longer periods). Other means could be pursued – arguably, the former UK government's proposals do not extend to management incentive plans for senior employees, and therefore it may be permissible to make the awards under such plans subject to non-competes which persist over a specific period. It remains to be seen, however, whether workarounds such as these will be possible.

When it comes to EU Member States, given the stringency of existing regulations and extensive case law, international employers must be cognizant of the non-unified legal landscape. Each post-termination non-compete agreement must continue to be carefully scrutinized to ensure compliance with the specific requirements and relevant case law of the applicable Member State. For instance, in Germany, despite the relevant codified law now being over 100 years old, new case law continues to contextualize and refine the way that the law in this area is applied. Therefore, it is crucial for employers to stay updated on the latest legal developments in each jurisdiction.

Chris Bracebridge
Employment
Partner, London
+44 20 7067 2063
CBracebridge@cov.com

Lindsay Burke
Employment
Partner, Washington
+1 202 662 5859
LBurke@cov.com

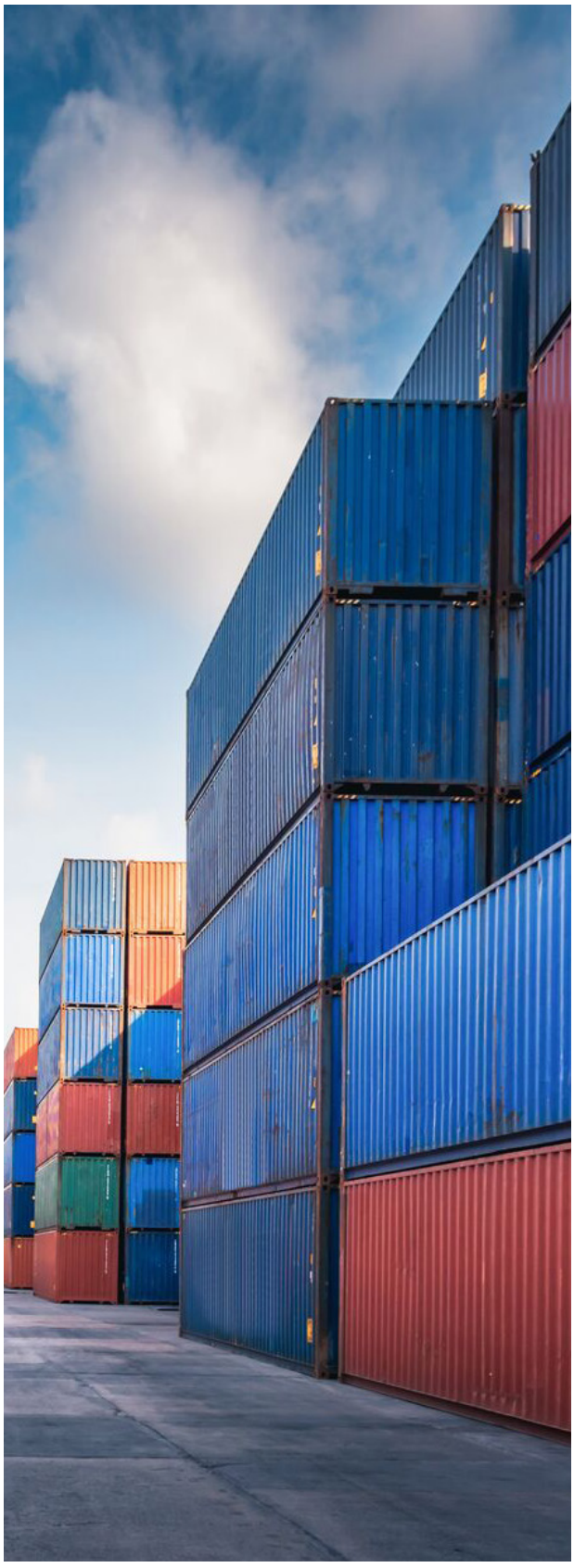
Evan Parness
Employment
Partner, New York
+1 212 841 1273
EParness@cov.com

Antonio Michaelides
Employment
Of Counsel, London
+44 20 7067 2027
AMichaelides@cov.com

Nadine Kramer
Employment
Of Counsel, Frankfurt
+49 69 768063 351
NKramer@cov.com

Jenna Wallace
Employee Benefits and Executive Compensation
Of Counsel, New York
+1 212 841 1093
JWallace@cov.com

U.S. Commerce Department Continues Revising Export Controls Enforcement and Voluntary Disclosure Policies



As part of the U.S. Commerce Department's ongoing overhaul of its export controls enforcement program and voluntary self-disclosure ("VSD") policies, on September 12, 2024, the Department's Bureau of Industry and Security ("BIS") announced a final rule (the "Rule") revising the administrative and enforcement provisions of the Export Administration Regulations ("EAR") to codify policy changes previously announced in various public memoranda, increase presumptive penalties by removing caps on the dollar-value starting point from which BIS calculates penalties for certain less serious violations of the EAR, provide BIS more flexibility in assessing penalties, and provide guidance on the Department's "General Prohibition Ten" process for authorizing activities relating to items that have been involved in violations of the EAR. The Rule is effective as of September 16, 2024. In addition, BIS announced that it had appointed its first-ever Chief of Corporate Enforcement, a former U.S. Department of Justice ("DOJ") prosecutor whose appointment underscores BIS's continued focus on bringing larger and more impactful enforcement cases against companies.

1 Revisions to Voluntary Self-Disclosure Policies and Penalty Guidelines

VSD Policies

Through the Rule, BIS is formally incorporating into the EAR certain policy changes that were previously announced in a series of public memoranda, and that were aimed at encouraging parties to submit VSDs. With these changes, BIS noted that "the regulations contain all relevant policies and procedures for submitting VSDs." The previously announced policy changes that have now been incorporated into the EAR include:

- Based on a historical, contextual, and teleological interpretation of Article 22 EUMR and the EUMR itself, NCAs cannot ask the Commission to examine transactions which do not meet their national thresholds.
- A "fast track" disclosure process for minor or technical violations that allows disclosing parties to submit shorter and less-detailed narrative accounts of the violations being disclosed, as well as guidance on the information required in those accounts;
- The option for BIS to impose non-monetary penalties in cases that are not egregious and have not resulted in national security harm, but rise above conduct warranting merely a (typically non-public) warning letter; and
- The addition of a party's deliberate decision not to disclose significant violations of the EAR as an aggravating factor when assessing whether a violation is egregious and setting an appropriate penalty.

In remarks at the Center for Strategic & International Studies on the day the Rule was announced, BIS Assistant Secretary for Export Enforcement Matthew Axelrod noted that, after announcing these policy changes, BIS saw a nearly 30 percent increase in disclosures of significant violations and a 20 percent increase in industry tips that led to actionable leads for agents in the field.

Penalty Guidelines

BIS has also revised the EAR's penalty guidelines to tie penalty amounts more closely to transaction values and provide BIS more flexibility when assessing aggravating and mitigating factors. Specifically, BIS eliminated previous dollar-amount caps for base penalties in non-egregious cases. Base penalties are dollar values that BIS sets as presumptive penalties, then increases or decreases based on aggravating and mitigating factors in each case. Base penalties thus serve as the starting point for penalty calculations. Before the Rule, base penalties for non-egregious violations were capped at $125,000 (if voluntarily disclosed) and $250,000 (if not voluntarily disclosed). The new Rule removes those caps, setting the base penalty for non-egregious violations at up to half the transaction value (if voluntarily disclosed) and up to the transaction value (if not voluntarily disclosed). BIS lays out these base penalty principles in a matrix, which has changed as follows:

Previous Base Penalty Matrix

	Egregious case	
Voluntary Self-Disclosure?	**No**	**Yes**
Yes	One-Half of the Transaction Value (capped at $125,000 per violation)	Up to One-Half of the Applicable Statutory Maximum
No	Applicable Schedule Amount (capped at $250,000 per violation)	Up to the Applicable Statutory Maximum

Revised Base Penalty Matrix

	Egregious case	
Voluntary Self-Disclosure?	**No**	**Yes**
Yes	Up to One-Half of the Transaction Value	Up to One-Half of the Applicable Statutory Maximum
No	Up to the Transaction Value	Up to the Applicable Statutory Maximum

Of course, neither the base penalty amount nor the ultimate penalty amount can exceed the applicable statutory maximum. The statutory maximum authorized under the Export Control Reform Act of 2018 is currently the greater of $364,992 or twice the value of the transaction.

In parallel, BIS has removed references to the percentage decrease amounts that previously generally applied to certain mitigating factors, in order to provide BIS more flexibility in its assessment of the impact that all factors may have on the appropriate penalty amount. BIS also clarified that appropriate penalty amounts could be higher or lower than the applicable base penalty, depending on the impact of all relevant factors, and in all cases will not exceed the statutory maximum.

In addition, BIS has also newly revised one existing aggravating factor and two general sub-factors used to assess penalty amounts. The Harm to Regulatory Program Objectives aggravating factor has been revised to include the enabling of human rights abuses as a specific consideration in assessing the impact of an apparent violation on U.S. foreign policy objectives. Separately, the Regulatory History and Criminal Conviction general sub-factors have been revised to allow BIS to consider, respectively: (1) antiboycott matters and regulatory compliance history prior to the five years preceding the date of the transaction giving rise to the violation as part of a respondent's regulatory history; and (2) as part of the respondent's criminal history, resolutions with the Justice Department other than a criminal conviction, including deferred prosecution agreements and non-prosecution agreements.

Finally, BIS removed language from the penalty guidelines regarding the practice of suspending or deferring a portion of a civil penalty if the suspended amount is applied to compliance program enhancements. BIS explained that "companies should independently make appropriate investments in their compliance program sufficient to identify and prevent potential violations, and generally should not expect to receive credit for the cost of making such investments against administrative penalties for past misconduct."

These changes, which will likely enable BIS to impose larger financial penalties on companies accused of export controls violations, form part of a longer-term effort by BIS to obtain more costly and demanding resolutions to enforcement cases.

2 Refinements to General Prohibition Ten Authorization Process

Earlier in 2024, in a policy memorandum, BIS announced a policy change to allow any person, not limited to parties submitting VSDs, to notify the Director of the Office of Export Enforcement ("OEE") of an export violation and seek authorization from the Office of Exporter Services ("OES") to engage in activities with respect to items involved in the violation. This change was significant, because most activities with respect to such items are prohibited under the EAR's General Prohibition Ten and EAR Section 764.2(e), and submitting a VSD was previously a prerequisite to applying for a waiver of that prohibition. The Rule codifies that relatively new policy into the EAR, allowing parties that have not been involved in an export violation but that are in possession of, or otherwise have an interest in, an item subject to General Prohibition Ten to seek a waiver to engage in further activities with respect to the item.

Additionally, the Rule revises the EAR to clarify that items subject to a violation may be returned to the United States upon notification to OEE and do not require further authorization for the return to the United States or future activities that comply with applicable EAR provisions after the initial return to the United States. BIS expects this change will reduce the administrative burden on industry and BIS by reducing the number and scope of waiver filings companies must submit and BIS must process.

3 Appointment of Chief of Corporate Enforcement

BIS also announced the appointment of Raj Parekh, a former Acting United States Attorney for the United States Attorney's Office for the Eastern District of Virginia, as BIS's first-ever Chief of Corporate Enforcement. In announcing the appointment, Assistant Secretary Matthew Axelrod described it as an important step in institutionalizing the efforts BIS has undertaken over the past three years to strengthen its administrative enforcement program.

This appointment advances BIS's longer-term project to bring former prosecutors to BIS and the Department of Commerce's Office of Chief Counsel for Industry and Security. It also parallels the appointment of Ian C. Richardson as the DOJ National Security Division's first Chief Counsel for Corporate Enforcement in September 2023. The two appointments reflect BIS and DOJ's continued interest in pursuing significant cases against companies.

We are closely monitoring developments concerning U.S. export controls and will issue further updates in the event of material developments. In the meantime, we would be happy to address any questions you may have. Covington's International Trade Controls team—which includes lawyers in the firm's offices in the United States, London, and Frankfurt—regularly advises clients across business sectors, and would be well-placed to provide support in connection with these new and proposed export controls developments, or to assist with comments on these proposed rules.

Covington's market-leading Trade Controls practice works seamlessly with our preeminent White Collar group, roster of former high-level U.S. government officials, and seasoned teams on the ground in China and around the globe to advise clients on their most sensitive and complex trade controls enforcement matters.

Our trade controls lawyers also work regularly with Covington's Global Public Policy team—consisting of over 120 former diplomats and policymakers in the United States, Europe, the Middle East, Latin America, Africa, and Asia—many of whom have had substantial government experience in sanctions and export controls matters, and who regularly advise our clients on emerging sanctions policy matters and related engagements with government stakeholders.

Peter Flanagan
International Trade
Partner, Washington
+1 202 662 5163
PFlanagan@cov.com

Kimberly Strosnider
Trade Controls Enforcement
Partner, Washington
+1 202 662 5816
KStrosnider@cov.com

Steven Fagell
Litigation and Investigations
Partner, Washington
+1 202 662 5293
SFagell@cov.com

Nancy Kestenbaum
Litigation and Investigations
Partner, New York
+1 212 841 1125
NKestenbaum@cov.com

Aaron Lewis
White Collar Defense and Investigations
Partner, Los Angeles
+1 424 332 4754
ALewis@cov.com

Peter Lichtenbaum
Litigation and Investigations
Partner, Washington
+1 202 662 5557
PLichtenbaum@cov.com

Eric Carlson
Litigation and Investigations / Anti-Corruption / FCPA
Partner, Washington
+1 202 662 5253
ECarlson@cov.com

Stephen Rademaker
Public Policy
Senior Of Counsel, Washington
+1 202 662 5140
SRademaker@cov.com

Corinne Goldstein
International Trade
Senior Counsel, Washington
+1 202 662 5534
CGoldstein@cov.com

Eric Sandberg-Zakian
Regulatory and Public Policy
Partner, Washington
+1 202 662 5603
ESandbergZakian@cov.com

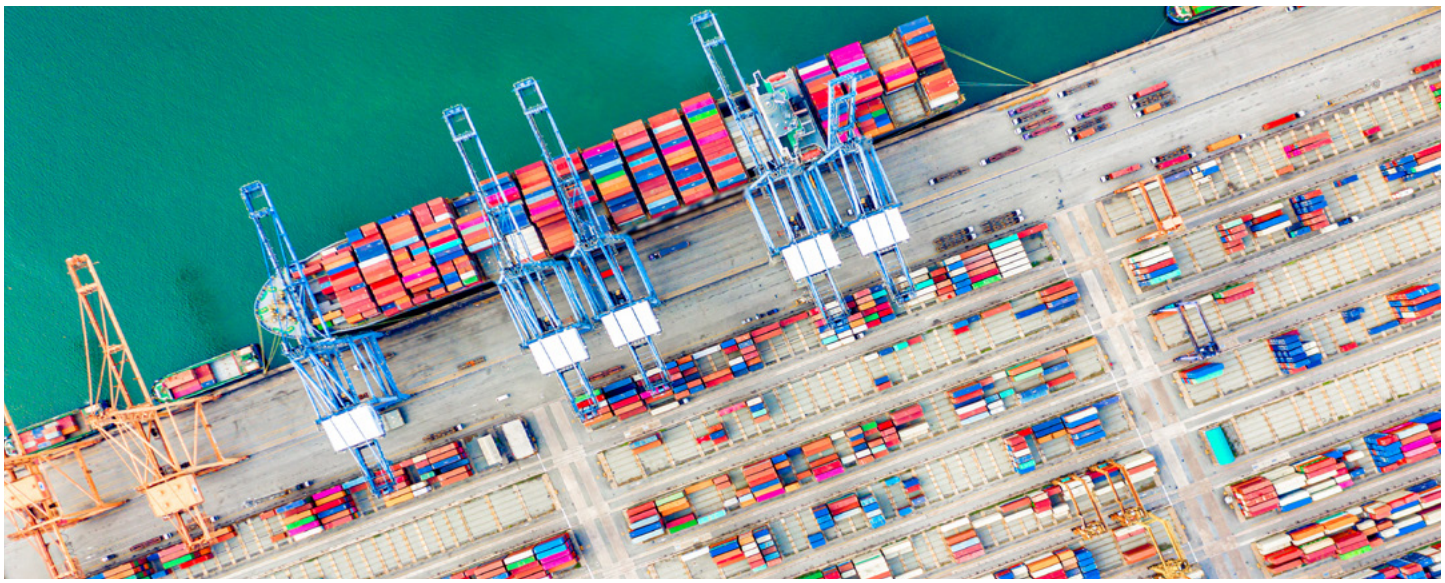
Joshua Williams
Litigation and Investigations
Partner, Washington
+1 202 662 5618
JNWilliams@cov.com

Seth Atkisson
International Trade
Special Counsel, Washington
+1 202 662 5781
SAtkisson@cov.com

Lisa Ann Johnson
International Trade
Associate, Washington
+1 202 662 5928
LlaJohnson@cov.com

Caroline Garth
International Trade
Associate, Washington
+1 202 662 5452
CGarth@cov.com

Shanelle Van
International Trade
Associate, Washington
+1 202 662 5532
SVan@cov.com



COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com