Nordic Newsletter

December 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!

We're excited to share the latest edition of our Nordic Newsletter!

This issue features Heather Finstuen, a partner in our Washington, D.C. office who focuses on cross-border investments and U.S. national security matters. Heather has extensive experience advising Nordic-based investors on strategic U.S. investments and navigating the CFIUS approval process.

Speaking of which, this edition also includes an article on FDI screening in the EU defense sector.

Additionally, our Washington, D.C. colleagues have developed a practical tool for dealmakers negotiating government contracts—don't miss it!

And of course, our newsletter wouldn't be complete without a look at the latest U.S. tariff enforcement trends.

We wish you and your loved ones a wonderful holiday season and look forward to opportunities to meet and work together in 2026. Enjoy the read!

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

New UK Employment Rights Bill - The Most Radical Employment Law Changes in a Generation

Creation of the Cross-Agency Trade Fraud Task Force and the Future of Tariffs Enforcement

August, September, and October 2025 Cybersecurity Developments Under the Trump Administration

Contractors Should Not Overlook the Administration's Call to Action on Commerciality

Eight Things Dealmakers Should Know About Government Contracts

Five Key Points on FDI Screening in the EU Defence Sector

Five major changes to the regulation of cybersecurity in the UK under the Cyber Security and Resilience Bill

Meet the Nordic Initiative:
Heather Finstuen

Who is Heather Finstuen?

I'm a native Californian and have lived in Washington D.C. for nearly 20 years. DC has wonderful museums, and my favorite is the National Portrait Gallery. It's also great place to raise a family, and we have two daughters who grew up here. I'm also proud to have Norwegian ancestry, with great-great-grandparents who emigrated from Oslo to the United States around 1875.

Tell us about your legal practice...

I'm a partner in our U.S. cross-border investment and national security practice and have been at Covington since starting as an associate in 2007. My practice focuses on guiding international and U.S. clients through U.S. national security reviews and approvals, which often occur in the context of transactions. It's a regulatory practice that moves at the fast pace of M&A, and stays interesting through the changing scope of the definition of national security and evolving technologies. I frequently advise on reviews by the Committee on Foreign Investment in the United States (CFIUS) and mitigation of foreign ownership, control, or influence (FOCI) by the U.S. Department of Defense and U.S. Department of Energy.

What inspired you to become a lawyer?

I was attracted to become a lawyer by the combination of strategic thinking, writing, and oral advocacy.

What do you like the most of advising Nordic-based clients?

My practice – which involves presenting clients and their businesses to U.S. national security regulators – requires that I learn about my clients' strategic goals, technology, and operations. I'm often a long-term advisor and I love learning about how Nordic companies have innovated and thrived and helping them achieve their business goals.

Your go-to Nordic restaurant / dish

Fika. I wish this was a U.S. tradition.

Favorite Nordic movie / music band

Abba, of course!

Licorice or kanelbulle?

Kanelbulle – just like my Grandma made.

Events

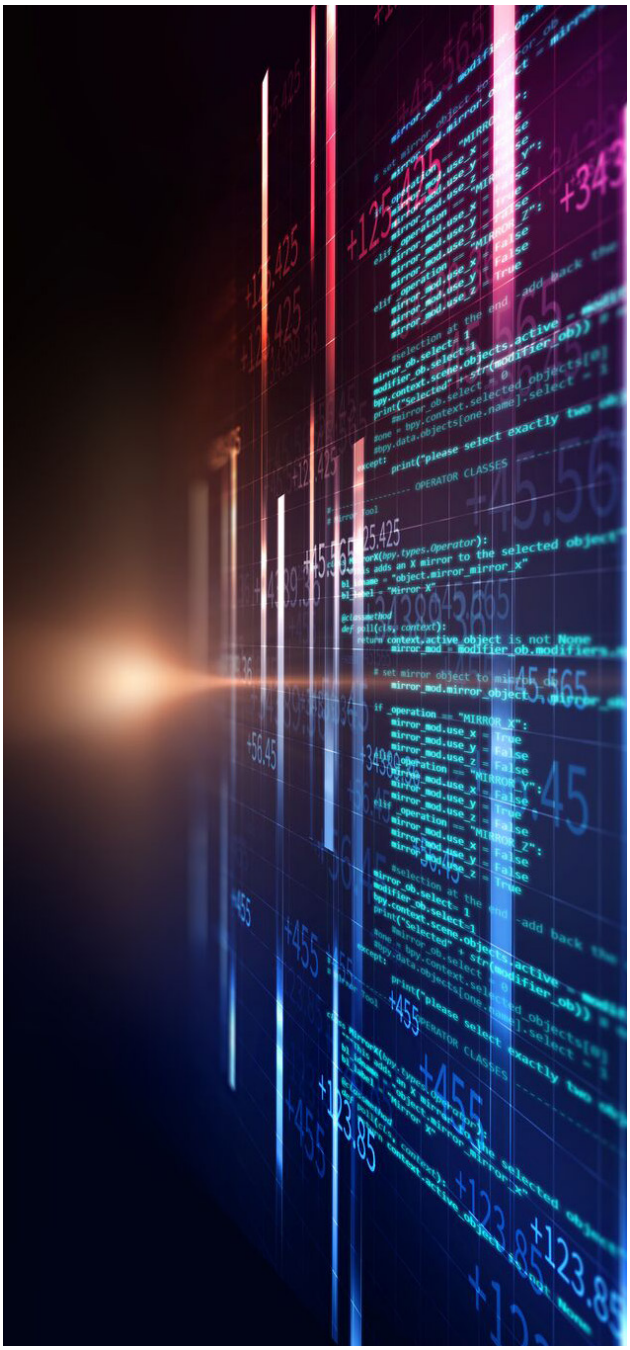
NORDIC WEBINAR SERIES:

Safeguarding Against Cyber And AI Risks

The global business landscape is undergoing a profound shift driven by technological advancements, increasing reliance on digital infrastructure, evolving regulatory environments, digital threats, and innovative measures to mitigate risk. Effectively navigating the complexities of legal and compliance risk in relation to the intersection of cyber and AI, requires diligence and strategic foresight.

In this webinar, Covington's industry-leading legal experts in cybersecurity and insurance provided guidance on key developments and compliance requirements in the EU, United States, and China and summarized essential insurance coverage strategies that are crucial for Nordic businesses seeking to secure their digital futures.

Watch Here



Topics Include:

- **Key Developments for Cybersecurity Regulation:** Explore key developments in the EU, United States, and China as it relates to cybersecurity compliance and reporting obligations.
- **The Future of AI and Cybersecurity Risks:** Cybersecurity risks and the potential impacts to AI.
- **Best Practices for Managing Global Cyber Incidents:** Discover effective incidence response strategies.
- **Strategizing for Nordic Contractual Risk Mitigation:** Analyse and implement insurance and indemnity practices to protect business interests.
- **Insurance Solutions:** Learn about the evolution of relevant insurance solutions and 'additional insured' status on policies issued to vendors.

Ashden Fein
Cybersecurity
Partner, Washington
+1 202 662 5116
AFein@cov.com

Marialuisa Gallozzi
Internet of Things
Partner, Washington
+1 202 662 5344
MGallozzi@cov.com

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

NORDIC WEBINAR SERIES:

Exploring the U.S. Defense Market Opportunities for Nordic Companies and Investors

The defense sector is experiencing a significant transformation, fueled by rapid innovation, changes in the defense industrial base, increased budgets, and evolving transatlantic partnerships. Nordic companies and investors, known for their cutting-edge technologies and strategic foresight, are positioned to capitalise on these opportunities. However, navigating the complexities of regulatory compliance and structuring of business engagements is key.

This webinar covered these dynamics, with guidance on entry pathways and compliance requirements crucial for Nordic suppliers and investors.

Watch Here

Topics Include:

- **Entry Strategies to Working with the U.S. Government:** Exploring effective pathways to working directly or indirectly with the U.S. government, such as setting up a U.S.-based subsidiary, teaming and subcontract arrangements, joint ventures, reseller arrangements, mergers & acquisitions, and directsales models.
- **Navigating U.S. Regulations:** Understanding compliance requirements, including key certifications, supply chain restrictions, and industrial security requirements.
- **Real-World Case Studies:** Reviewing successful entry of companies into the U.S. market, highlighting best practices and lessons learned.

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

Brian Yang
Corporate / M&A
Partner, Washington
+1 202 662 5576
BYang@cov.com

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

New UK Employment Rights Bill

The Most Radical Employment Law Changes in a Generation:

The Employment Rights Bill ("**ERB**"), first introduced in October 2024 as part of the new Labour government's "*Make Work Pay*" initiative (see our previous article on this here), is edging closer to becoming law. Once passed, the ERB will implement radical changes affecting all UK employers for many years to come.

Initially expected to pass in summer 2025, the ERB has undergone numerous amendments, which have now pushed it back to at least the end of 2025 (potentially passing any day now). Even its headline proposals are still undergoing change, with ministers making a significant announcement last week that, instead of eliminating the two year qualifying period for unfair dismissal entirely, the period will instead be shortened to six months.

This client alert is the first in a series that we will release over coming years, to help our clients navigate the lengthy implementation period needed to introduce all of the sweeping new rights under the ERB.

1 When Will the New Rights Apply?

Once enacted, the ERB will become effective in phases, starting in late 2025 through to at least 2027. The Government's "Roadmap for Implementation" outlines this provisional timeline.

Some limited measures, especially those concerning trade unions, will come into effect shortly after the ERB passes (potentially late 2025). The next major milestone will be in April 2026. In this alert, we focus on four notable changes set to take effect in April 2026: "day 1" paternity leave and unpaid parental leave; enhanced whistleblowing protections; the maximum collective redundancy protective award doubling; and the establishment of the Fair Work Agency.

2 Key Changes on the Horizon (April 2026)

"Day 1" Paternity Leave and Unpaid Parental Leave

The ERB will make paternity leave and unpaid parental leave "day 1" rights by removing their minimum service requirements. It will also allow employees to take paternity leave and pay even after they have already taken shared parental leave and pay, which is not currently the case. Although the practical effects of this may be limited since statutory paternity leave is still only two weeks long and parental leave remains unpaid, employers will still need to review and update their family leave policies in response to these changes.

Enhanced Whistleblowing Protections

Under the ERB, complaints of sexual harassment will now be recognised explicitly as a form of whistleblowing (provided that they meet the public interest test and other legislative criteria) by being added to the list of "qualifying disclosures". While the change may have limited practical impact since many such complaints will already be protected under existing health and safety grounds, the Government is clearly emphasising the importance of treating these complaints seriously and trying to encourage their reporting. Employers will need to review their whistleblowing policies and reporting channels in light of this change.

Maximum Collective Redundancy Protective Award Doubling

Employers contemplating large-scale redundancies (note that the threshold for this is also set to change under the ERB) should be aware that the maximum protective award for failing to meet collective consultation requirements will double, to 180 days' pay per employee. This enhanced penalty may reduce the incentive for employers to pay employees in lieu of proper collective consultation and significantly increases the financial risks of non-compliance.

Establishment of Fair Work Agency

The Fair Work Agency, a new public authority with wide powers to enforce labour market regulations and bring employment tribunal proceedings on behalf of workers, will also be established in April 2026.

3 Consultation, Consultation, Consultation

It is important to note that much of the ERB serves as framework legislation, which will be shaped by statutory codes of practice and secondary legislation requiring further consultation. Accordingly, the Government has set out an extensive schedule of consultations, which started in Autumn 2025 and will focus on: a shorter qualifying period for unfair dismissal rights; trade union measures; fire and rehire; bereavement leave; rights for pregnant workers; and ending the exploitative use of zero hour contracts. We will be monitoring these consultations closely, as these aspects of the new laws take shape.

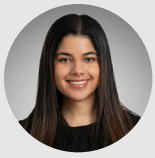
4 What Happens Next?

As it approaches the final stages of the UK parliamentary process, it is increasingly important – particularly for HR and compliance teams – to familiarise themselves with the contents of the ERB. This may involve scheduling training sessions, preparing for policy reviews and developing internal action plans. The phased implementation of the ERB should make this process more manageable, but the piecemeal nature of ongoing consultations and secondary legislation will require employers to remain alert to ongoing changes over the next two years. If you have questions about the ERB, or any other employment matters, we are happy to assist with any queries.

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

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

Richard Rowlands
Employment
Associate, London
+44 20 7067 2210
RRowlands@cov.com



Salena Mann
Employment
Associate, London
+44 20 7067 2156
SMann@cov.com

Contractors Should Not Overlook the Administration's Call to Action on Commerciality

In November 2025, Secretary Hegseth delivered a speech at the National War College introducing transformations to the defense procurement process. Among them, the Secretary discussed awarding companies bigger and longer contracts for proven systems; removing "excessive and burdensome" requirements (for example, acquisition rules, accounting standards, and testing oversight); and empowering program leaders with authority to direct program outcomes, move money, and adjust priorities. Overall, the speech outlined a vision for a more agile defense procurement process that leans heavily on practices already proven and featured in the commercial sector.

Additionally, the Secretary emphasized that the Department of Defense ("DoD") should prioritize acquiring commercial products and services. The Secretary promised a forthcoming policy that would require commercial procurement at DoD as a first resort. Specifically, he explained:

[T]oday at my direction, commercial products and offerings will be the default policy. We will enhance the presumption of commerciality. Within 90 days, we will issue guidance that demands a commercial first and alternative proposals policy to enhance flexibility.

The Secretary explained that DoD's push for commercial solutions would be accompanied by increased flexibility to negotiate solutions that do not meet 100% of program requirements. He noted that DoD would prioritize industry-driven, commercial solutions first, "even if that means bids that do not meet every requirement." He further stated, "we will be open to buying the 85% solution and iterate together over time to achieve the 100% solution." The Secretary's speech comes just over six months after President Trump signed Executive Order ("EO")

14271 on Ensuring Commercial, Cost-Effective Solutions in Federal Contracts. As we detailed in a prior blog post, the EO directed the Federal Government to procure commercially available products and services to the maximum extent practicable, consistent with the preference for commercial procurement already codified in statute. Among other things, the EO introduced a procurement review process to ensure that agencies consider using commercial procurement for acquisitions and provide a justification for using a non-commercial product or service. Given the Administration's continued emphasis on commercial procurement, contractors of all sizes are well advised to take stock of their products and services to determine whether they could potentially fulfill commercial criteria. FAR 2.101 defines what it takes for a product or service to qualify as commercial.

For instance, if a contractor offers products, the contractor should consider whether its products are "of a type customarily used . . . for purposes other than governmental purposes," and have been offered for sale, lease, or license to the general public. And if a contractor offers services, the contractor should consider whether its services are (i) procured in support of commercial products and are provided to the general public under terms similar to those offered to the Federal Government, or (ii) "of a type offered and sold competitively in substantial qualities in the commercial marketplace based on established catalog or market prices" under standard commercial terms and conditions. Contractors may find that products or services they previously considered non-commercial could, with some adjustments or better documentation, be justified as commercial solutions. The Administration's drive for commercial solutions could benefit contractors that can adjust quickly. As has always been the case, FAR Part 12, commercial item contracting imposes a less daunting suite of acquisition regulation flow-downs. And now, in the context of the Administration's push for procuring commercial solutions as a first resort and requiring agencies to justify using non-commercial procurements, contractors that can transition to providing commercial solutions could enjoy a significant selling advantage over contractors that persist in offering non-commercial solutions. The Secretary's recent speech reflects an intent to move quickly in reforming DoD's acquisition process, and contractors that are able to quickly pivot to providing commercial solutions where none previously existed could be well positioned to take advantage of new opportunities. We will continue to watch for updates as the Administration's effort to reform the government's acquisition process unfolds.

Scott Freling
Government Contracts
Partner, Washington
+1 202 662 5244
SFreling@cov.com

Daniel Raddenbach
Government Contracts
Associate, Washington
+1 202 662 5743
DRaddenbach@cov.com

Five Key Points on FDI Screening in the EU Defence Sector

The war in Ukraine, and other recent geopolitical conflicts, has underscored the need for EU-based defence capabilities to scale up to face these challenges. Several EU initiatives which have sought to stimulate investment are starting to bear fruit, as the European Defence Agency recently reported record high defence spendings in the EU (€350bn for 2024, a 19% increase to 2023). Political support for the sector has been demonstrated by Commission President Von Der Leyen proclaiming *"a new era for European Defence and Security"* in her latest State of the European Union address. In this context, understanding the regulatory framework applicable to investments in the EU defence sector is proving increasingly important. Foreign direct investment ("FDI") screening regimes represent one of the most important regulatory checks to clear for investors. This blog post reviews **five key points for investors to consider** when making investments in the defence sector given the current geopolitical context.

1 Stricter jurisdictional triggers

Many EU Member States' FDI regimes have specific, and generally stricter, rules for the defence sector. There are three features which contrast with the general rules applicable to other sectors:

- **More investors caught:** Specifically, non-domestic investors (and sometimes even domestic investors) are more likely to be caught by the FDI regimes. Germany's FDI regime, for example, extends its screening to non-German investors where the target is active in the defence sectors, whereas its FDI rules relevant to all other sectors only cover investments by non-EU investors.
- **More investments caught:** Low shareholdings (typically 10%, or even less as low as 3% in Italy) and indirect investments in defence-sector targets (e.g. of a non-domestic entity with a domestic subsidiary) are more likely to be in scope. For example, Hungary triggers on indirect investments of at least 10% in the defence sector (whereas it otherwise typically applies only to direct investments).

- **Separate reviewing authority:** Investors in defence targets may have to make a separate (and sometimes additional) filing with the Ministry of Defence specifically (e.g. in Spain), as opposed to the Ministry of Economy for the general regime.

2 Unequal jurisdictional triggers

Whilst there are some relatively clear-cut lines to determine what characterizes a defence activity that falls within scope of an FDI regime (e.g. Tier 1 OEMs manufacturing military equipment), the assessment can become a lot more complex depending on how far up the supply chain a target is located. In turn, this is important because not all EU FDI regimes define "defence" the same way, which results in uneven jurisdictional triggers:

- **Sensitive contracts:** Some regimes require the target to have contracts with sensitive customers (e.g. military customers or Tier 1 OEMs) and go further and require the contracting party to be a local entity of the target (e.g. France).
- **Sensitive supplies:** Some regimes capture suppliers of goods on the EU's common military and/or dual-use lists, regardless of the contractual position or whether the goods are in fact used for military/defence applications (e.g. Spain). To complicate further, EU Member States' FDI regimes diverge on which "list" they use as a reference point: the older EU regulation of dual-use products (e.g. France), the newer EU regulation (e.g. Ireland), or a mixture of EU regulation and their own domestic regulation (e.g. Germany).
- **Sensitive activities:** Some regimes capture only specific activities taking place locally (typically manufacturing, research, and development activities) (e.g. Germany or France), while others will capture any "activity" (which can be read to include export supplies into the country) (e.g. Belgium or Italy). Not all regimes define what "activities" are considered to be sensitive, which (given the often-sparse guidance to the contrary) can lead to a counterintuitive interpretation that non-sensitive products or services (e.g. janitorial/catering services to (e.g.) Tier 1 OEMs) are "sensitive activities" for FDI purposes.
- **Sensitive access:** Some regimes will capture targets with access to sensitive facilities (e.g. military installation) or their IT infrastructure, regardless of the products or services supplied (e.g. Germany). Similarly, having certain security clearances can suffice to automatically trigger a regime (e.g. Norway).

  Consequently, investors must tailor their due diligence to both the target's local presence in a given jurisdiction, but also potentially its customer base.

3 Impact of target activities on substantive review

The substantive considerations will vary depending on the scale of the target and their importance to the national defence of their home EU Member State. This bears out in three particular areas:

- **Security of supply:** Generally, arguments that a transaction does not result in security of supply concerns are easier to evidence for smaller players, provided they are not themselves a sole supplier into a critical project (e.g. with a unique technological input). Conversely, suppliers providing NATO-certified items that can be easily obtained from other NATO suppliers, will typically not raise as many issues.
- **Maintenance of R&D efforts:** Where a target is an established local player, it may have benefitted from significant government funding related to sensitive national

projects over the years. Investments in these players will therefore more likely involve remedies or commitments surrounding these projects, which could take the form of continued (or even increased) R&D expenditure and guarantees surrounding continuity of the research, potential routine on-site monitoring, etc.

- **Domestic strategy on national security:** Investors should also diligence whether their target – whilst not currently being a "national champion" – is being positioned to become one by virtue of its innovative technology, and/or the amount of government funding it has received. This could be the case where the technology remains in early-stage development but shows high growth potential specifically for the defence sector. Authorities may be less willing to unconditionally approve a transaction involving a national champion (or a potential national champion) by their foreign competitors, out of concern that national capabilities will be diminished at the profit of foreign competition.

4 Impact of investor nexus on substantive review

For the defence sector, FDI authorities will typically be particularly sensitive to the existing capabilities and geographical footprint of the investor. For example:

- **Transaction-related exposure to extraneous trade controls restrictions:** Authorities will be concerned with whether a non-EU foreign investor acquiring an EU target will expose that EU target to the buyer's home jurisdiction export controls, which could make it harder for the target to continue to supply its existing customers. For example, the United States International Traffic in Arms Regulations ("ITAR", part of the US export control regime) can have such an impact on EU targets because they apply globally to a group (including its EU subsidiaries). Given the US export control interests are not always aligned with EU's, an EU target that becomes subject to ITAR due to a foreign investment could result in key components or technologies becoming subject to a third country's export control legislation. Managing such interactions and interdependencies with foreign regulations requires carefully balanced mitigation plans.
- **Government-mandated information sharing:** Authorities will scrutinize whether a foreign investor can be forced by its home jurisdiction to hand over information of its foreign subsidiaries. This could result in foreign government piercing the corporate veil and gaining access to sensitive technology currently being developed or manufactured in the EU. Screening authorities will seek to understand what physical and virtual barriers are or can be put in place to protect the EU target's sensitive information. These may involve separate boards, firewalls, or even golden shares to ensure no undue interference takes place.
- **Ties or supplies to hostile nations:** Authorities will assess whether buyer have themselves problematic/sensitive supplies. For example, if an investor supplies arms to customers/countries that are hostile to the country screening the investment, the screening authority may block the investment owing to perceived negative impact on public security, or at least apply in-depth scrutiny and request more invasive remedies.

5 Reputation and relationships matter

Investors with an established reputation in the jurisdiction where an FDI screening review takes place may face lower scrutiny compared to new or lesser-known investors. This can result in less onerous – or no – remedies being required. Leveraging an investor's positive reputation requires a careful mix of advocacy and factual evidence. For example where an investor already (i) holds contracts relating to sensitive in-country technology and has a good track record of compliance with the applicable regulations regarding treatment of security classified information, (ii) has senior personnel and staff within with similar degree of clearance as the target, or (iii) demonstrates existing capabilities to create and maintain virtual and physical barriers, it would

likely prove better positioned for a favourable outcome and getting its investment through.

Conversely, a purely financial investor with no track record in the defence sector and limited exposure to the relevant jurisdiction might face greater scepticism and scrutiny from the reviewing authorities. This could in turn translate into more burdensome commitments to obtain clearance, as well as a longer clearance timeline.

These factors will be particularly relevant for acquisitions organized in a tender process.

Conclusion: Strategic Actions for Investors

Investors in the EU defence sector can consider the following actions to facilitate the FDI assessment and review of their proposed investments:

- **Special Regimes Demand Thorough Due Diligence:** Delve deeply into the regulatory environment, mapping out defence definitions and jurisdiction-specific challenges, including broader definitions of "foreign investor" and investment types.
- **Evaluate Security of Supply and National Champion Status:** Analyse whether your investment involves a national champion or is critical to national security.
- **Assess Investor's Government Nexus:** Investigate how relations with foreign governments might impact your investment, especially regarding export control laws. Consider geopolitical macro dynamics and the potential extraneous political interferences.
- **Leverage Reputation and Relationships:** Build trusted relationships and positive reputation with local authorities.

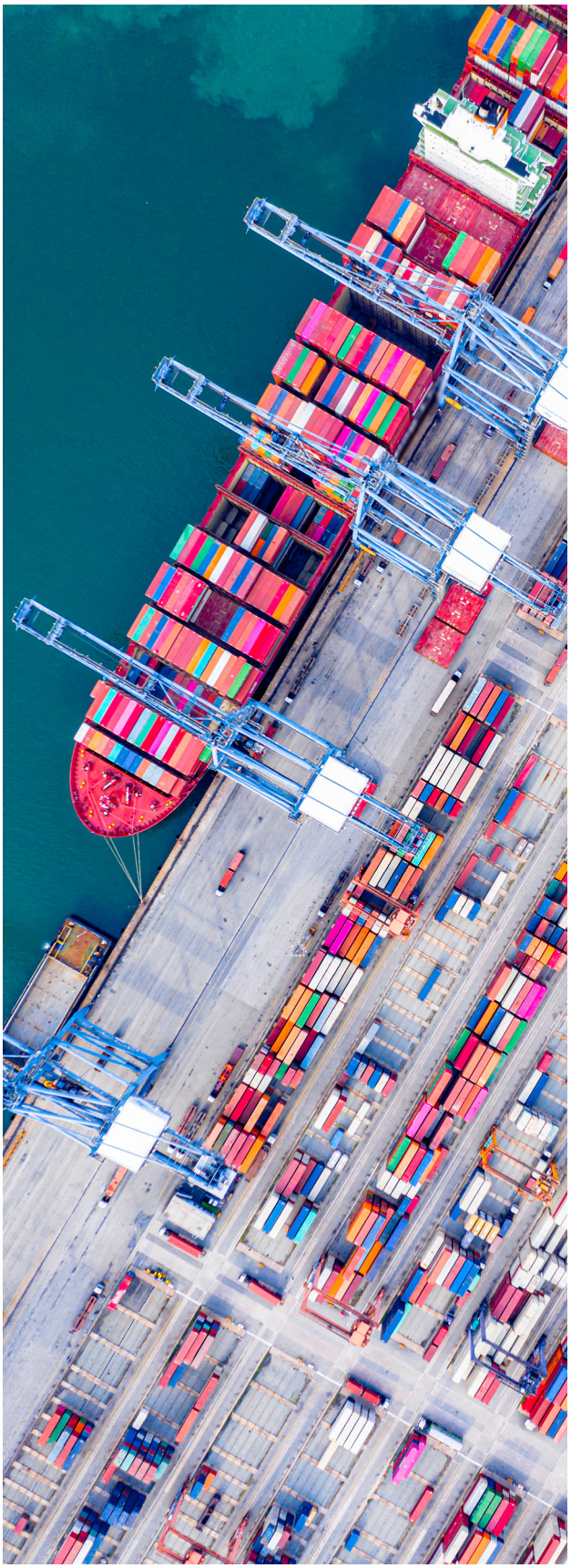
Covington can guide and support investors at each of these steps, building from its deep FDI expertise and cross-practice capabilities.

James Marshall
Antitrust / Competition
Partner, London
+44 20 7067 2280
JMarshall@cov.com

Laurie-Anne Grelier
Antitrust / Competition
Of Counsel, Seoul
+82 2 6281 0005
LGrelier@cov.com

Romain Girard
Foreign Direct Investment Regulation
Associate, Brussels
+32 2 545 7510
RGirard@cov.com

Creation of the Cross-Agency Trade Fraud Task Force and the Future of Tariffs Enforcement



On August 29, 2025 the Department of Justice ("DOJ") announced the launch of a cross-agency Trade Fraud Task Force ("TFTF"), a partnership between DOJ's Civil and Criminal Divisions, as well as the Department of Homeland Security ("DHS"). On the same day, the U.S. Court of Appeals for the Federal Circuit ("Federal Circuit") issued a 7-4 ruling striking down President Trump's use of the 1977 International Emergency Economic Powers Act ("IEEPA") to impose tariffs, a decision which, if ultimately upheld, would limit the administration's trade fraud enforcement efforts.

The creation of the Task Force is a significant development that furthers the Administration's efforts to prioritize enforcement focused on tariff evasion. Importers, and any of their corporate affiliates involved in U.S. trade activities, should remain diligent and ensure compliance with all appropriate regulations in this heightened enforcement environment. And, to comply with the current U.S. trade and customs regime, importers must continue to pay IEEPA tariffs, as the Federal Circuit decision will not take effect until the Supreme Court has weighed in.

This article introduces the Task Force and its origins; describes the Task Force's new features and likely impact on enforcement; explains the Federal Circuit ruling finding the IEEPA tariffs to be in excess of the President's authority; explores the effect of this opinion on the current trade landscape; highlights repercussions for noncompliance with the trade regime; and concludes with recommendations for navigating trade compliance going forward.

What is the Trade Fraud Task Force?

The TFTF is a partnership between DOJ and DHS that will "aggressively pursue enforcement actions against any parties who seek to evade tariffs and other duties, as well as smugglers who seek to import prohibited goods into the American economy."[1] The Task Force will address the Administration's concerns about non-compliance with trade laws, stemming from the "America First Trade Policy" announced on Inauguration Day. The TFTF's creation is consistent with DOJ's practice of forming special task forces to address high concern areas.

Trade fraud has not historically been a primary focus of criminal enforcement by DOJ, but DOJ announced a renewed interest in this space in its May 12 white collar enforcement plan, which described the Division's enforcement priorities as including "trade and customs fraud, including tariff evasion."[2]

What's New?

The TFTF's rollout is still in its early stages, and it remains to be seen what approaches the Task Force will take to identify and investigate trade fraud. However, the DOJ Press Release highlights several areas of increased emphasis.

- First, the TFTF places increased emphasis on the role of domestic industries as key partners in its effort to root out trade fraud. The TFTF believes U.S. companies are often best placed to spot fraud due to their direct involvement in the markets and competitions where trade fraud occurs. Therefore, the TFTF encourages companies to refer potential offenders and cooperate with the TFTF to help bring offenders to justice.
- Second, the TFTF seeks to enhance enforcement by "augment[ing] the existing coordination mechanisms" between DOJ and DHS. In particular, the TFTF seeks to facilitate greater communication and harmonization among the DOJ Civil Division, DOJ Criminal Division, DHS Customs and Border Protection, and DHS Homeland Security Investigations. Although the details are still unclear, DOJ believes that the "enhanced cooperative efforts will serve the dual purposes of a more efficient government for the taxpayer and improved enforcement and deterrent outcomes."
- Third, DOJ wants to assume a more active role in detecting and prosecuting trade fraud. While there were numerous civil trade fraud resolutions in 2025, those matters were initiated by *qui tam* whistleblowers or voluntary disclosures. However, on the same day the Criminal Division announced its new enforcement priorities, it also amended its Corporate Whistleblower Awards Pilot Program to reflect that an individual may be eligible for a whistleblower award if they provide information that leads to criminal or civil forfeiture exceeding $1,000,000 for "trade, tariff, and customs fraud" by a corporation, among other priority areas. This incentivizes whistleblowers to come forward with trade and customs fraud allegations without having to file a *qui tam* action.

Unlike some prior task force announcements, which have been accompanied by the launch of a supporting website with additional guidance and materials, thus far DOJ has provided limited information to the public about the TFTF. Companies and contractors should continue to monitor the rollout for new developments.

Risks of Non-Compliance for Corporations – Criminal and Civil Penalties

The formation of the TFTF will increase the resources devoted to enforcement against trade and customs fraud and will potentially drive up the number of investigations, the stakes of which have always been high.

Trade and customs fraud enforcement in the past often has been driven by civil reverse False Claims Act cases brought by DOJ in coordination with Customs and Border Protection (CBP). Penalties in these cases can be substantial because under the FCA, a court can impose treble damages and additional penalties ranging from $14,308 to $28,619 per violation. However, and particularly with the creation of the TFTF, DOJ may seek to bring more criminal trade and customs fraud cases under a range of criminal statutes, including federal laws prohibiting smuggling (18 U.S.C § 545), wire fraud (18 U.S.C. §§ 1343, 1349), and false statements (18 U.S.C. § 1001).

Companies that willfully underpay certain tariffs also could be subject to criminal penalties and fines under the IEEPA, assuming the president's invocation of IEEPA to levy those tariffs is upheld. Civil violations of IEEPA-based tariffs can be significant (up to twice the value of the transaction) and are enforced on a strict liability basis, as opposed to civil recoveries under the False Claims Act, which require proof of knowledge or reckless disregard.

Strict Liability May No Longer Apply to Tariff Evasion

With the creation of the TFTF on the same day as the issuance of the Federal Circuit ruling striking down the IEEPA tariffs, importers may be wondering if these tariffs are still binding and whether the TFTF can penalize nonpayment of these duties. The answer to both questions is yes – for now.

The Federal Circuit decision involved two types of tariffs: the "Trafficking Tariffs" (tariffs enacted against Mexico, Canada, and China for alleged failure to meaningfully address the trafficking of opioids into the United States) as well as the "Reciprocal Tariffs" (10 to 50 percent ad valorem tariffs on nearly every country which does significant trade with the United States in response to a supposed lack of reciprocity in trade relationships).

The Federal Circuit affirmed the Court of International Trade's May ruling, finding the far-reaching Trafficking and Reciprocal Tariffs to exceed "IEEPA's grant of presidential authority." The Court held that while IEEPA "bestows significant authority on the President to undertake a number of actions in response to a declared national emergency," this power does not extend to the "unheralded" and "transformative" tariffs enacted by the President.

Despite this opinion, it would be premature to celebrate an end to the IEEPA tariffs. The Government has already appealed the ruling to the Supreme Court. If the Supreme Court were to accept the appeal, it could take months for the matter to be resolved. And even if the Supreme Court were to deny the appeal or otherwise let the ruling stand, the Federal Circuit's ruling would not immediately block the imposition of the IEEPA-based tariffs. Rather, the ruling remands the decision to the lower court for further consideration of the appropriate relief. Thus, at minimum, we are months away from a final decision determining the fate of the IEEPA tariffs.

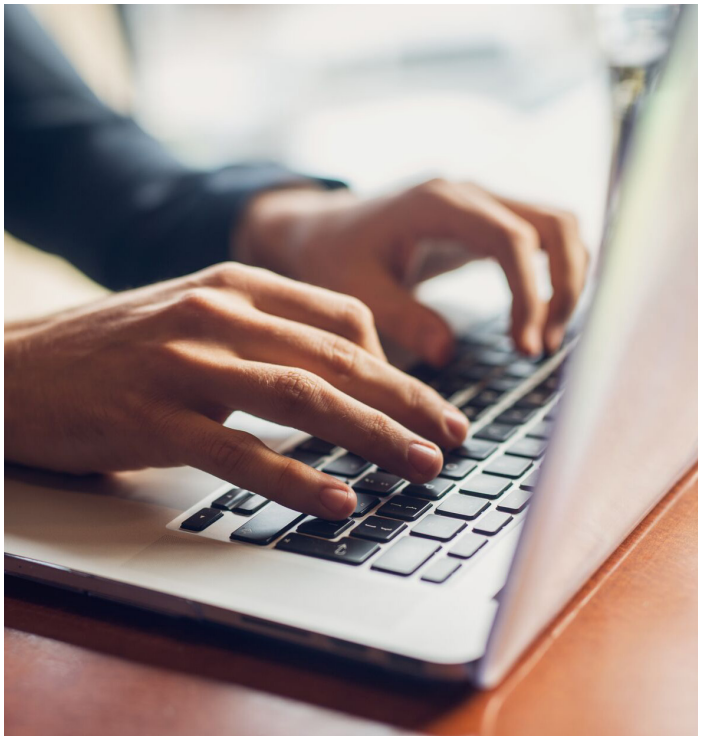
Recommendations

With the increased emphasis on trade fraud enforcement, and given the complex and shifting customs and trade landscape, companies should be taking steps now to protect themselves from potential risks. Key mitigation measures include:

- **Audit your importing practices.** The current tariff landscape is ever evolving and creates special challenges for companies and contractors that are not historically accustomed to aggressive enforcement in this space. Companies—especially those with substantial importing footprints—would be well-served by engaging in audits of its current practices to identify and remediate potential gaps.
- **Create or enhance your trade compliance program.** DOJ has historically indicated a willingness to mitigate penalties and damages—including the use of possible deferred prosecution agreements—for companies with effective compliance programs. In September 2024, DOJ's Criminal Division released guidance on how it evaluates corporate compliance programs, which was the subject of a separate Covington client alert found here. At a high-level, a good corporate compliance program meets three criteria: (1) it is

well designed; (2) it is adequately resourced and empowered; and (3) it works in practice. An investment in compliance is a worthwhile step to avoiding and mitigating possible investigations. However, CBP has recently shown less of an inclination to mitigate penalties, an approach encouraged by the Trump Administration. We will publish a client alert focused on this topic shortly.

- **Track updates to applicable tariffs.** New tariffs are being imposed and challenged at a breakneck pace. It is crucial companies monitor all such announcements to avoid owing hefty penalties. It is also recommended that companies consult counsel to ensure appropriate entry of goods such that importers are taking advantage of all helpful customs programs and thus avoid overpaying tariffs.
- **Encourage reporting of, and then promptly investigate, potential trade misconduct.** A good trade compliance program has a trusted mechanism that allows employees to anonymously report allegations of impropriety. Companies should also create robust procedures for investigating allegations of misconduct, and where appropriate, implementing discipline or corrective actions. Strong internal reporting procedures can help mitigate the risk of *qui tam* whistleblowers and increase the opportunity for the Company to course correct problems before they compound.



Alexander Chinoy
Litigation and Investigations
Partner, Washington
+1 202 662 5559
AChinoy@cov.com

Mona Patel
Litigation and Investigations
Partner, Boston
+1 617 603 8804
MPatel@cov.com

James McCall Smith
Litigation and Investigations
Partner, Washington
+1 202 662 5550
JMsmith@cov.com

Ariel Rosenbaum
Litigation and Investigations
Associate, Washington
+1 202 662 5365
ARosenbaum@cov.com

Michael Pierce
Government Contracts
Associate, Washington
+1 202 662 5728
MPierce@cov.com

Binx Saunders
Litigation and Investigations
Associate, Washington
+1 202 662 5497
ESaunders@cov.com

Julia Shults
International Trade
Associate, Washington
+1 202 662 5492
JShults@cov.com

Pearson Goodman
International Trade
Associate, Washington
+1 202 662 5664
PGoodman@cov.com

Eight Things Dealmakers Should Know About Government Contracts

The bottom line:

- Government contracting has many nuances and unique features that require extra attention from dealmakers.
- The much publicized in-progress overhaul of Federal Acquisition Regulations will remove some burdens on companies that sell products or services to the US government.
- But government contracting is—and will remain—a highly regulated industry and successful M&A deals involving contractors often require specialized expertise from lawyers who are well versed in the regulations that apply to government contracting.

Government contracting—historically viewed as relatively stable—has encountered novel challenges and opportunities in the first several months of the Trump administration. Even in the face of uncertainty from executive actions, public sector-focused businesses continue to be a fertile ground for mergers and acquisitions activity.

We are seeing an increased emphasis on companies leaning into the administration's focus on commerciality, rapid deployment of technology, and openness to creative contracting mechanisms. And investors are putting significant capital behind those strategies. As many savvy private equity firms have known for some time, companies that serve the US government, either as a prime contractor or as a subcontractor, can be attractive acquisition targets because of historically stable customer demand and consistent cash flow.

However, deals involving government contractors carry their own complexities. The industry is highly regulated, and effective dealmakers should understand the specific challenges and compliance requirements that companies face when they do business with the US government. These risk factors continue to evolve as the Trump administration embarks on an overhaul of federal contracting regulations and seeks to cut through perceived regulatory red tape.

1 Government Contracts Differ from Commercial Contracts

Contracts awarded by the US government, and subcontracts issued in support of those prime contracts, typically have a laundry list of Federal Acquisition Regulation clauses and other regulatory provisions that inform the rights and obligations of the parties.

The Trump administration's ongoing overhaul of the acquisition regulation looks to relax or even eliminate some of these compliance obligations, but many such requirements are ingrained by statute and will remain. And certain foundational precepts of government contracting won't change.

For example, the government has an automatic right to terminate most prime contracts for its convenience and to make unilateral changes to the scope of work and other contract terms. The government's obligations, particularly in multi-year contracts, often are subject to the availability of appropriated funds.

This means that an acquisition target's contracts need to be evaluated for the favorability of their written terms, as well as for the status of performance, funding, customer relationship, and competitive dynamics.

2 Government Contracts Often Aren't Freely Assignable Assets

Under the Anti-Assignment Act, a contractor can't assign a prime contract with the US government without approval from the customer. This prohibition often isn't addressed anywhere in the four corners of the contract.

Instead, the prohibition and the administrative process for seeking government approval are addressed in Subpart 42.12 of the FAR, which requires the assignor to submit the request for approval after it has executed the instrument effecting the assignment to the assignee. In an asset sale, the parties generally must seek post-closing approval from the government to effectuate at least part of the transaction.

This means that transaction parties typically must establish an interim arrangement to govern performance of the contracts between closing and novation, a period that can extend for at least several months.

3 Government Contractors Must Share Detail About Their Ownership

The US government expects contractors to, at minimum, disclose their immediate owner and their highest-level owner.

Traditionally, the Defense Counterintelligence and Security Agency and other national security agencies have required companies holding security clearances to complete more extensive ownership disclosures. This includes submitting a full organizational chart and identification of foreign equity holders with interest of 5% or more, even if they're entirely passive.

More recently, we have seen an uptick in procuring agencies, such as the Department of Energy, requiring disclosure of foreign affiliates even when no industrial security issues are implicated. DCSA also is developing a pre-award entity vetting process for companies that don't hold clearances, which will subject many more defense contractors to extensive ownership disclosures.

4 Foreign Involvement Can Require Review and Mitigation

If DCSA or another US government agency determines that cleared contractor is subject to foreign ownership, control, or influence, the contractor must mitigate the FOCI to the government's satisfaction.

The required form of mitigation will depend on the nature of the FOCI and could range from a simple board resolution to a much more significant proxy agreement, which may require that governance responsibility and voting rights be placed in the hands of individuals who aren't connected to the company or its owner and who are approved by the government.

DCSA's upcoming pre-award entity vetting process for uncleared defense contractors will also assess FOCI and determine whether mitigation is required. In addition, regardless of whether a contractor holds a clearance, it may be necessary or advisable to present the transaction for pre closing review by the Committee on Foreign Investment in the United States. A CFIUS review can significantly lengthen the time between signing and closing and can result in mitigation obligations.

5 Permits and Other Governmental Authorizations Can Become Relevant

For any deal, it is important to get a handle on the permits and other governmental authorizations that an acquisition target relies on to conduct its business and the applicable regulatory framework for each authorization.

This is particularly true for deals involving a government contractor. For example, many government contractors in the defense and national security space must maintain a registration with the Department of State under the International Traffic in Arms Regulations. The ITAR requires State Department notification in connection with, among other things, a change of ownership or control of a registrant. For foreign buyers, there is an additional pre-closing notification requirement under the ITAR that can have implications for closing timeline.

As another example, if a company engages in certain activities regulated by the Federal Communications Commission or otherwise holds FCC licenses, it often must obtain FCC approval prior to effecting a change of control.

6 There Are Many Socioeconomic Preferences

The US government has established socioeconomic preferences in several aspects of the procurement process to try to boost participation from small businesses, including those owned by women, veterans, and those considered socially and economically disadvantaged.

Many prime contracts are awarded on a set-aside basis, meaning that only eligible businesses are permitted to compete for the contract. Likewise, small businesses are exempted from having to maintain a small business subcontracting plan or to comply with the Cost Accounting Standards.

Where an acquisition target relies on small business or other preferential status, it is prudent to confirm during due diligence that past claims to this status make sense, including that they account for the size of the target and each of its affiliates.

This is a tricky area of compliance and continues to attract significant enforcement attention from the Department of Justice, even as the administration has shown skepticism regarding certain socioeconomic preference programs. It is also important to consider whether the proposed transaction will frustrate the acquisition target's ability to claim such status going forward, to hold on to previously awarded contracts, or to continue to pursue certain bids for new contracts.

7 There Are Specialized Accounting Requirements, Cost Disclosure Obligations, and Government Audits

Many government contractors must adhere to unique accounting and disclosure practices, which can be a source of historical liability and affect a buyer's post-acquisition plans.

For example, where applicable the Cost Accounting Standards require a company to align its accounting to a set of government standards, disclose how it accounts for particular costs, and engage with the government before making certain accounting practice changes.

The Truthful Cost and Pricing Data statute obligates certain contractors to provide certified cost or pricing data to justify its proposed pricing for a contract. In fulfilling those obligations, contractors sometimes must provide their government customer with information that reveals anticipated margins.

Regardless of whether these accounting or disclosure requirements apply to an acquisition target, however, it may still be subject to government audits and other compliance reviews. This scrutiny can result in repayment obligations and other liability.

8 Contractual Non-compliance Can Lead to Enforcement Action

Ordinary compliance matters in government contracting can quickly spiral into something much larger, such as a whistleblower action or a government investigation.

The False Claims Act permits the DOJ, or a private party, to pursue treble damages and statutory penalties against a company or other person that submits a false claim for payment to the US government. We have seen a substantial uptick in the use of the FCA to police contractor compliance with contract terms.

For example, the DOJ has been actively using the FCA to pursue cybersecurity-related non-compliance by government contractors since the Biden administration announced the Civil Cyber Fraud Initiative in 2021. And this past May, the DOJ launched a Civil Rights Fraud Initiative that said it aimed to use the FCA to investigate and "pursue claims against any recipient of federal funds that knowingly violates federal civil rights laws."

We expect FCA enforcement against government contractors, including in complex regulatory areas such as supply chain and cybersecurity compliance, will be a priority area of the DOJ for many years.

About the Authors

Scott Freling and Nooree Lee are partners in Covington's Government Contracts practice.

They focus their practices on guiding buyers and sellers—including a number of leading private equity firms—through the regulatory aspects of complex M&A deals involving companies that sell products or services to government customers. They have each served as the lead government contracts counsel in dozens of M&A deals, with a combined value of more than $80 billion. In addition, Scott and Nooree represent civilian and defense contractors in traditional government contracts matters, including compliance counseling, government investigations, audits, and disputes.

Scott co-chairs the firm's Government Contracts practice, and has been recognized by *Chambers USA* as a leading practitioner in this space. Nooree recently was recognized by the *Washington Business Journal* with a "40 Under 40" Award.

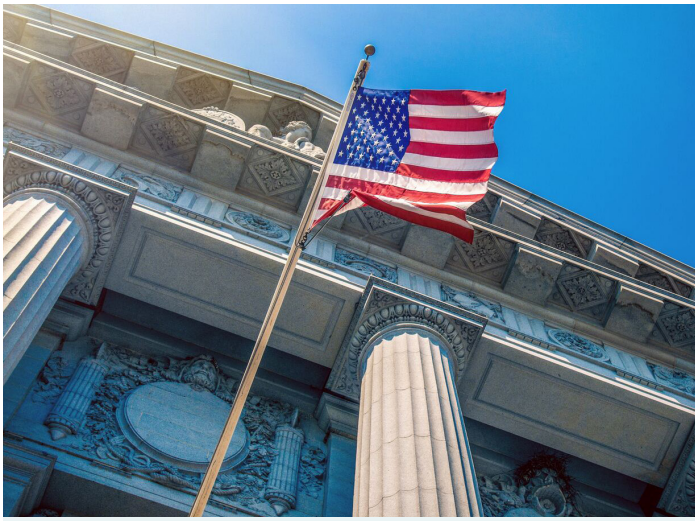
Covington
Government Contracts

Chambers TOP RANKED USA 2025

Elite Band 1- Government Contracts

Scott Freling
Government Contracts
Partner, Washington
+1 202 662 5244
SFreling@cov.com

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



Key Takeaways

With the interplay of regulatory approvals, unique compliance obligations, and potential for government scrutiny and enforcement, government contracts M&A demands specialized expertise. Early and informed risk identification is a critical component of due diligence on public sector-focused businesses.

Without proper planning, regulatory complexity can erode value, lead to mid-deal surprises, or leave open significant post-closing exposure. Most representations and warranties insurers are sensitive to the range of possible losses at issue in deals involving a government contractor, and they typically identify regulatory compliance as a focus area for underwriting.

This complexity is particularly acute today, with the pace of regulatory change in the government contracts industry moving at hyperspeed. At the same time, the Trump administration's "art of the deal" approach to government contracting may give a significant edge to companies positioned to lean into the administration's policy priorities.

This all calls for nuanced business and legal diligence into how companies approach their sales to the US government.

Five major changes to the regulation of cybersecurity in the UK under the Cyber Security and Resilience Bill

As the UK Government has recognized, cyber incidents—such as Jaguar Land Rover, Marks and Spencer, Royal Mail and the British Library—are costing UK businesses billions annually and causing severe disruption. The Government recognizes that cybersecurity is a critical enabler of economic growth ("we cannot have growth without stability"), and that the current laws have "fallen out of date and are insufficient to tackle the cyber threats faced by the UK." Accordingly the UK Government this week published its long-awaited Cyber Security and Resilience Bill (the "**Bill**"), which will amend the existing Network and Information Systems Regulations 2018 (the "**NIS Regulations**"), and grant new powers to regulators and the Government in relation to cybersecurity.

The NIS Regulations are the UK's pre-Brexit implementation of Directive (EU) 2016/1148 (the "**NIS Directive**"), which established a "horizontal" cybersecurity regulatory framework covering essential services in five sectors (transport, energy, drinking water, health, and digital infrastructure) and some digital services (online marketplaces, online search engines, and cloud computing services). EU legislators replaced NIS Directive in 2022 with the "NIS2" Directive, which Member States were meant to transpose into national law by October of last year (although many are still late in doing so. See our post on NIS2 here for an overview of the requirements of NIS2).

The Bill is the UK's effort at modernizing the framework originally set out in the NIS Directive. In its current form, the Bill will:

- Significantly expand the scope of the NIS Regulations—to cover, among other things, data centers and managed service providers—and impose additional substantive obligations on covered organizations.
- Increase potential fines—up to GBP 17m or 4% of the worldwide turnover of an undertaking—and extend the powers of competent authorities to share information with one another, issue guidance, and take enforcement action.
- Establish a framework for future changes to the NIS Regulations, mechanisms for competent authorities to impose specific cybersecurity requirements on covered organizations, and greater Government direction of cybersecurity matters.

Below, we set out further detail on five major changes in UK cybersecurity regulation arising from the Bill.

1 Data center operators—among others—will now fall within scope of the NIS Regulations

At present, the NIS Regulations cover two types of covered entities—"operators of essential services" ("**OESs**," including the main types of critical infrastructure, such as energy, transport, and water providers) and "digital service providers" ("**DSPs**," specifically cloud computing, online search engines, and online marketplaces). The Bill will expand the scope of the OES designation to cover providers of data center services that offer a rated IT load of more than 10 megawatts, and are provided "on an enterprise basis." The Bill's definition of "data centre service" broadly follows the equivalent definition in NIS2 but is more detailed; in essence, it covers the provision of data center space and supporting infrastructure (e.g., utilities and security infrastructure). This differentiates data centre providers from cloud computing providers, which are already regulated as a DSP under the NIS Regulations. (Note that the definition of a "cloud computing services" will also be amended) The Secretary of State for Science, Innovation and Technology, along with Ofcom, will be the competent authority for regulating data center providers.

The Bill will also expand the scope of the NIS Regulations to cover:

- "Large load operators" in the electricity sector as OESs; and
- Managed service providers as a new category of operator with similar obligations to DSPs under the existing NIS Regulations. Interestingly, the definition of a "managed service provider" is more specific than the equivalent definition in NIS2. The Information Commission (which will soon replace the existing Information Commissioner's Office) will be the competent authority for managed service providers.

2 More incidents will be reportable, and the Government reserves the right to impose more specific security requirements

At present, the NIS Regulations require OESs to report to competent authorities any incident that "has a significant impact on the continuity of the essential service which that OES provides" to its competent authorities, taking into account factors such as the number of affected users, the duration of the incident, and the geographical area affected. DSPs must report incidents that have a "substantial impact on the provision of" any of the digital services they provide. It's fair to say, however, that authorities have not been overwhelmed: according to the Government's impact assessment, in 2019, 2020 and 2021, there were only 13, 12 and 22 NIS incidents reported, respectively.

The Government considers that this is because the definition of a significant incident has been too narrow. The Bill will expand the types of incidents that are reportable, in some cases extending to incidents that have had or are likely to have a "significant impact" in the UK. Generally, reportable "incidents" will include incidents that are "capable of" creating adverse impacts—not just those that have an actual such effect. However, covered entities will need to review the definitions of incidents carefully to understand what is reportable, because there are slightly different thresholds for different categories of provider.

For example, data center providers must report incidents that could have had, have had, are having or are likely to have, a significant impact on the operation or security of the network and information systems at issue, a significant impact on the continuity of the data center service, or any other significant impact.

In addition, the Bill will impose an obligation on OESs, DSPs, and managed service providers to notify customers that are likely to be "adversely affected" by the incident, taking into account the level of any disruption, any impact on that customer's data, and any impact on their other systems.

Although the Bill does not set out new substantive security requirements on covered entities, it empowers the Government to impose such requirements, including for national security purposes.

3 The Bill attempts to address supply chain security for OESs by creating a new category of "critical suppliers"

The Bill would permit competent authorities responsible for overseeing OESs and DSPs to designate—subject to a consultation process—"critical suppliers," i.e., individuals or organizations that rely on network and information systems to provide goods or services to an OES or DSP, for whom an incident would have the potential to cause disruption to the provision of an essential service that is likely to have a "significant impact on the economy or day-to-day functioning of society" in the UK.

As drafted, the Bill does not impose specific obligations on critical suppliers. However, such suppliers may, among other things, be the subject of directions from the UK Government to take steps in relation to the security of their services, or the subject of cybersecurity codes of practice from the Government. The Government has recognized that third-party service providers can create significant risks for OESs, DSPs, and managed service providers, and left itself flexibility to regulate further in the future. In addition, organizations (or individuals) can be designated as critical suppliers by multiple competent authorities (e.g., if they provide services to OESs in multiple different sectors). In recognition of this, the competent authorities are required to coordinate with one another in relation to designation decisions.

4 Increased fines and enhanced powers for competent authorities

The headline is that the level of potential fines is significantly increased: the cap for the most serious infringements will be the higher of GBP 17m or 4% of the worldwide annual turnover of an undertaking.

Ongoing infringements of requirements imposed by competent authorities can also be subject to daily penalty payments until they are rectified.

The Bill also empowers competent authorities to share information related to incidents among themselves, with law enforcement, with GCHQ, and with OESs, DSPs, managed service providers, and critical suppliers where necessary (although any such information sharing with private entities may not prejudice the security interests of others), and also with foreign competent authorities.

The Bill would also amend the NIS Regulations to set out in more detail the powers of competent authorities to demand information from covered providers, carry out inspections, and take enforcement action.

Competent authorities are also empowered to charge covered entities to cover the costs arising from the exercise of the authority's functions, subject to charging "schemes" that competent authorities may develop (subject to consultation with the organizations they regulate).

5 The UK Government will be empowered to take a more active role in cybersecurity regulation in the future

Parts 3 and 4 of the Bill establish a framework for the UK Government to set both the broad strategic direction for competent authorities' oversight and enforcement of cybersecurity, and to impose more granular obligations on covered providers.

At a high level, and among other things, the Bill would:

- require the Government to maintain a statement of its strategic priorities in relation to cybersecurity;
- empower it to pass secondary legislation requiring certain organizations to take specific cybersecurity measures and/or to grant new powers to competent authorities;
- as set out above, empower the Government to impose—in certain circumstances—specific cybersecurity requirements on all types of entities covered by the NIS Regulations, as well as other entities the Government chooses to designate. This includes a framework for imposing obligations on providers for national security purposes; and
- empower it to issue codes of practice setting out more detail on the measures covered providers could take to comply with their obligations under the NIS Regulations.

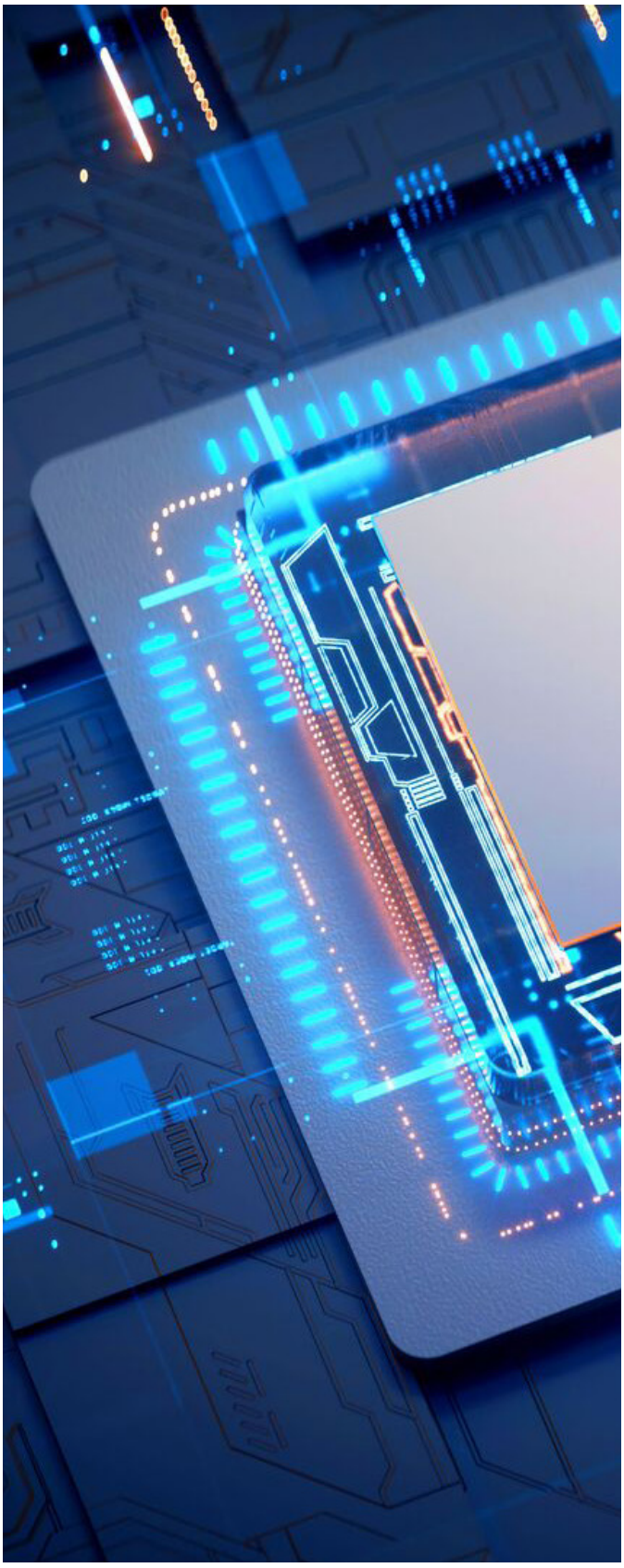
About the Data Privacy and Cybersecurity Practice

The Data Privacy and Cybersecurity Practice at Covington has deep experience advising on privacy and cybersecurity issues across Europe, including on the NIS Regulations, NIS2, and other cybersecurity laws. If you have any questions about how the Cyber Security and Resilience Bill will affect your business, or about developments in the cybersecurity space more broadly, our team would be happy to assist.

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

August, September, and October 2025 Cybersecurity Developments Under the Trump Administration



This is the seventh blog in a series of Covington blogs on cybersecurity policies, executive orders ("EOs"), and other actions of the Trump Administration. The sixth blog is available here and our initial blog is available here. This blog describes key cybersecurity developments that took place in August, September, and October 2025.

NIST Publishes Second Draft of Foundational Cybersecurity Activities for IoT Product Manufacturers (NIST IR 8259)

On September 30, National Institute of Standards and Technology ("NIST") released the second public draft of its NIST Internal Report ("IR") 8259, Foundational Cybersecurity Activities for Internet of Things ("IoT") Product Manufacturers. This publication outlines foundational cybersecurity activities and serves as a guide for IoT manufacturers to bolster the cybersecurity of their IoT products. The goal of the publication is to allow manufacturers to meet both regulatory standards and customer needs for secure deployment of their products. Key updates include the inclusion of "Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture," emphasizing the necessity for manufacturers to embed cybersecurity considerations throughout their product development processes. This activity addresses the need for a robust internal cybersecurity posture to protect both IoT products and the organizational systems. The draft also details the introduction of new activities tailored to better define IoT product cybersecurity capabilities, focusing on aligning these capabilities with customer needs and goals. Manufacturers are encouraged to use industry frameworks, such as NIST's Cybersecurity Framework ("CSF") and Risk Management Framework ("RMF"), to evaluate and mitigate risks. Additionally,

guidance on secure software development and supply chain risk management has been expanded, referencing NIST Special Publication ("SP") 800-161 Rev 1. The draft underscores the importance of continuous communication about software updates and product support to aid customers in maintaining IoT product cybersecurity throughout its lifecycle, including guidelines for end-of-life product management and decommissioning.

Cybersecurity Maturity Model Certification (CMMC) Program Procurement Final Rule Announced

On September 10, 2025, DoD published the final version of the Cybersecurity Maturity Model Certification ("CMMC") Defense Federal Acquisition Regulation Supplement ("DFARS") Procurement Rule ("Procurement Rule" or "Rule") in the Federal Register. We wrote about the Rule in more detail here. This Rule imposes the contractual requirements associated with the CMMC Program Rule that was published in final form in October 2024. The Procurement Rule will become effective sixty days after publication, on November 10, 2025 and will be implemented in a phased approach.

The CMMC Program is expected to have significant impacts on the federal supply chain, imposing certification requirements on all contractors and subcontractors with DoD contracts that include the relevant DFARS clause (currently DFARS 252.204–7021) and under which Federal Contract Information and/or Controlled Unclassified Information is processed, stored, or transmitted on contractor information systems. We have developed a toolkit of additional resources on CMMC available here.

CISA Delays Cyber Incident Reporting Rule for Critical Infrastructure

The U.S. Cybersecurity and Infrastructure Security Agency ("CISA") plans to delay the publication of its much-anticipated cybersecurity incident reporting rule implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). We wrote about this update here. According to an entry on the Spring 2025 Unified Agenda of Regulatory and Deregulatory Actions, released on September 4, 2025, CISA currently plans to publish the Final Rule sometime in May 2026, and it likely will not go into effect until sometime afterwards. As discussed in a previous blog post, CIRCIA established two cyber incident reporting requirements that are broadly applicable to covered entities in one of the 16 U.S. critical infrastructure sectors. When the Final Rule goes into effect, covered entities will be required to report covered cyber incidents within 72 hours of discovery and covered ransom payments within 24 hours. CISA published the Notice of Proposed Rulemaking ("Proposed Rule") on April 4, 2024, and the statute required CISA to publish the Final Rule within 18 months of the Proposed Rule. Accordingly, the Final Rule was previously expected to arrive by October 2025.

Cybersecurity Information Sharing Act of 2015 Allowed to Sunset

The Cybersecurity Information Sharing Act of 2015 ("CISA 2015"), which provided protections for sharing cybersecurity threat information with the federal government and others, officially sunset on September 30, 2025 pursuant to the law's original sunset date after efforts to re-authorize it did not succeed. We wrote about this update here. The law created a cybersecurity information sharing framework and established certain protections – including disclosure under FOIA, limits to liability, and limits to waiver of legal privilege – for sharing that information with private parties and the federal government. While the expiration does not prohibit industry participants from ongoing or future sharing of cyber threat information with the federal government and others, private sector companies can no longer rely on the liability protections in CISA 2015 when doing so.

Although several bills had been introduced in recent months to re-authorize CISA 2015's protections, including some that would have adjusted or altered CISA 2015's provisions, none of the bills significantly progressed before the current U.S. government shutdown. Going forward, organizations that share cyber threat information should consider how the absence of CISA 2015's protections might impact their sharing practices and monitor for future legislative efforts to re-authorize CISA 2015 or create a similar replacement framework for information sharing.

NIST Releases Long Awaited Revision to the Digital Identity Guidelines

On August 1, NIST announced the release of SP 800-63 Revision 4, Digital Identity Guidelines, which can be found here. This update comes after four years of drafting and thousands of public comments. The stated goal of the release is for the updated guidelines to "make navigating the digital world more secure and convenient." It explains that "a digital identity is intended to establish trust between the holder of the digital identity and the person, organization, or system interacting with the online service" and notes that online services require secure digital identity solutions to be secure themselves. NIST explained that the new guidelines intend to "respond to the changing digital landscape" since its last revision in 2017. NIST intends for this revision to focus on risk management adapted from real-world lessons learned. Some of the major changes include expanded fraud requirements, identity proofing processes, controls for deep fakes, and changes to the password composition and rotation expectations. It is possible that agencies could choose to incorporate some or all aspects of these guidelines into contracts for the acquisition of software services and, ultimately, contractors who are required to comply with the Digital Identity Guidelines will need to ensure their services comply with the requirements of Revision 4.

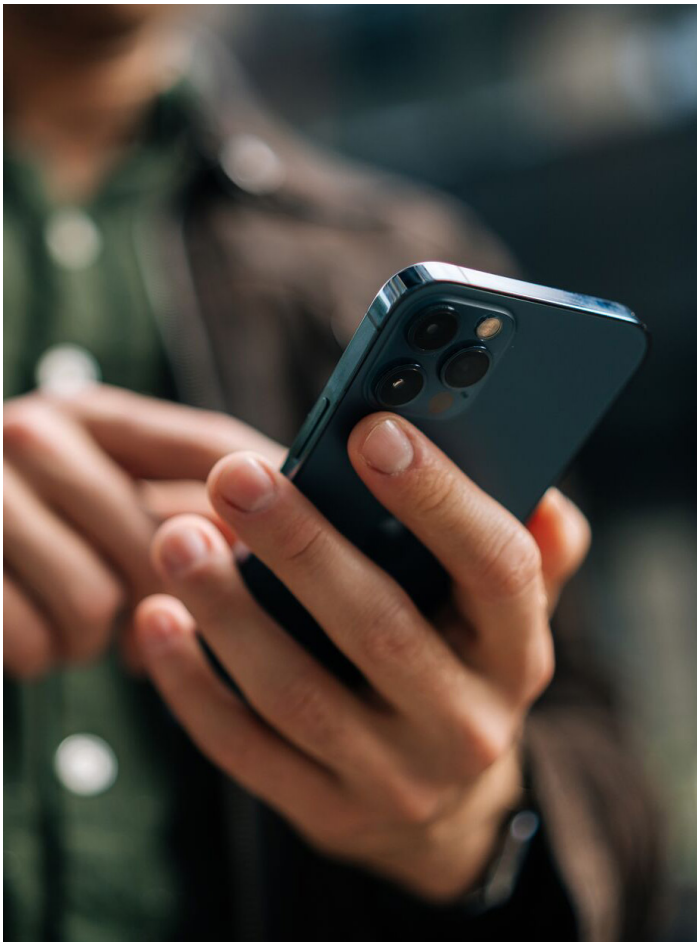
CISA Updates Guidance for Minimum Elements of Software Bills of Materials

On August 25, CISA announced the release of draft guidance for 2025 Minimum Elements for a Software Bill of Materials ("SBOM"). This has initially been released as a draft here. As background, the first SBOM minimum elements guide was released in 2021 in response to a Biden administration EO. CISA was seeking feedback on the draft guidance and published its request for comment here. The new minimum elements aim to reflect expanded capabilities and advancement of SBOM tooling since the inception of the guidance in 2021. Although not required by law, CISA hopes that these new minimum elements will continue to promote SBOMs as a way to provide information to software users and to better inform supply chain risk management in their software supply chains.

NIST Internet of Things Internal Report

On August 25, the NIST National Cybersecurity Center published the final version of the NIST IR 8349, Methodology for Characterizing Network Behavior of IoT Devices that it announced here.

The report works in tandem with the Cybersecurity Center's project Securing Home IoT Devices Using Manufacturer Usage Description ("MUD"), through which companies create MUD profiles for their IOT devices and a companion "MUD-PD" tool released by NIST to help with the characterization of IoT devices. The goal of the report is to create a system for characterizing IoT devices to enable a better understanding of IoT device network behavior, which will allow for the more effective implementation of appropriate network access controls, such as firewall rules or access control lists.
The report walks through the new network traffic capture methodology that is used for the MUD profile, then discusses the various use cases, network communications, and privacy implications of devices.



New NIST Cryptography Standard for Small Devices

On August 13, NIST finalized SP 800-232, Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions, here. This document identifies four recommended cryptography standards specifically adapted for small devices, which NIST describes as ready for use to protect data created and transmitted by IoT devices. These algorithms require less computing power and time than more conventional cryptographic methods. NIST envisions that this will protect information created and transmitted by billions of devices of IoT devices as well as other small electronics, such as RFID tags and medical implants.

Susan Cassidy
Data Privacy and Cybersecurity
Partner, Washington
+1 202 662 5348
SCassidy@cov.com

Ashden Fein
Data Privacy and Cybersecurity
Partner, Washington
+1 202 662 5116
AFein@cov.com

Robert Huffman
Data Privacy and Cybersecurity
Senior Of Counsel, Washington
+1 202 662 5645
RHuffman@cov.com

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

Krissy Chapman
Data Privacy and Cybersecurity
Associate, Washington
+1 202 662 5764
KChapman@cov.com

Grace Howard
Data Privacy and Cybersecurity
Associate, Washington
+1 202 662 5303
GHoward@cov.com

COVINGTON

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

www.cov.com