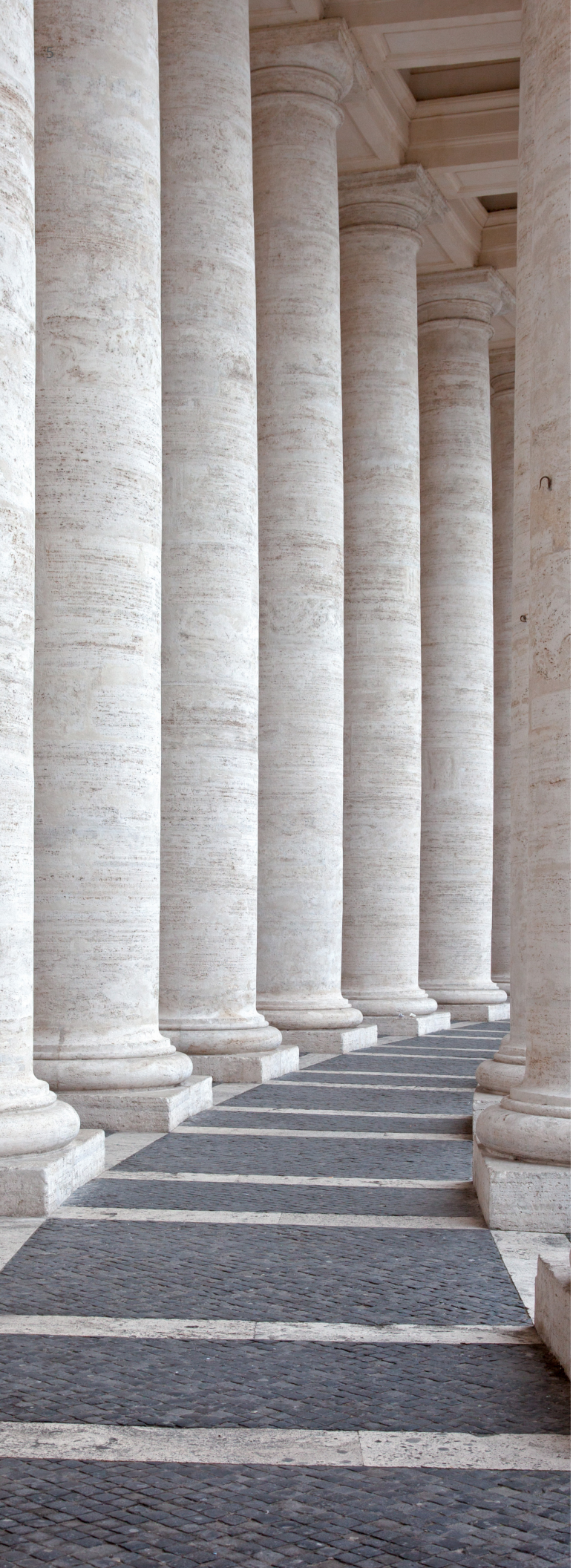
ADG Insights

U.S. government's increased efforts in supply chain integrity

Supply Chain Series, Volume 1
August 2018

Hogan Lovells



The U.S. government is pursuing several measures aimed at supply chain integrity.

Both the legislative and executive branches of the U.S. government are growing increasingly concerned with the issue of supply chain risks. The concern is not new, but there is now a realization that the issue must be dealt with aggressively in order to avoid severe damage to our national security. The reports of Russian infiltration onto the networks of the electric grid, the evidence of Russian interference with U.S. elections, and the reported exfiltration of hundreds of gigabytes of underwater warfare data from a contractor underscore that theoretical vulnerabilities do not stay theoretical; they can be manifested in real world consequences and in vulnerabilities that adversaries could exploit at their choosing.

A. The U.S. government is keenly focused on bolstering supply chain security

There is an escalatory risk of inaction – that is, there is a danger that failing to impose consequences on those who are probing and attacking the cyber infrastructure will convey the impression that such actions take place in a zone of impunity, which could lead to ever more damaging and destructive attacks. Some commentators predict that, at some point, the U.S. will feel compelled to respond with armed force because no other response will seem adequate in relation to the harm imposed by a malicious actor. Addressing supply chain risks is one way to reduce the escalatory risk of inaction because it makes malicious actors less likely to succeed.

Based on concerns and discussions over the course of several years, in recent testimony before the House Armed Services Committee the Department of Defense (DoD) announced a "Deliver Uncompromised" initiative. The initiative is:

> *focused on industry delivery of capabilities, services, technologies, and weapons systems that are uncompromised by our adversaries from cradle-to-grave. It aims to establish security as a fourth pillar in acquisition, on par with cost, schedule, and performance, and to create incentives for industry to embrace security, not as a "cost center," but as a key differentiator.*[1]

The Deliver Uncompromised initiative received additional attention on 13 August 2018 when The Mitre Corporation (which operates federally-funded research and development entities) published "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War." The purpose of the report is to "aid in the formation of a holistic strategy for dealing with supply chain security" within DoD, and to that end it suggests 15 distinct courses of action, including 1) elevate security to a primary metric in DoD acquisition and sustainment; 2) better coordinate intelligence throughout the federal government on supply chain issues by forming a National Supply Chain Intelligence Center; 3) establish independently implemented automated assessment and continuous monitoring of Defense Industrial Base (DIB) software; and 4) require industry-standard information technology practices in all software developments.

Some of these measures are directed to the government itself, such as better coordinating intelligence throughout the government. Likewise, the recommendation to establish automated assessment and continuous monitoring of software developed by the DIB would be a task for the government – though one that might be extremely difficult to do well. A tool that can assess and monitor the performance of software for security flaws or for malicious conduct certainly would be helpful in providing for improved security, but developing such a tool that can be applied at scale is no small challenge. Other recommendations would impose significant burdens on contractors, but at this point it is unclear what those burdens would be, and what imposing those burdens would accomplish.

What should contractors be expected to do? How can new security requirements be shaped to ensure that the gain to the government is worth the pain to the contractors, which will inevitably cause pain to the taxpayers by way of increased costs? There is a need for a robust dialogue between government and the contractor community based on a mutual understanding that: 1) the issue of supply chain security is critical to national security; 2) it is an extremely difficult problem to address; and 3) crafting a solution that takes the complexity and difficulties fully into account is essential to effectively address the problem.

1 *See* https://docs.house.gov/meetings/AS/AS00/20180621/108468/HHRG-115-AS00-Wstate-BingenK-20180621.pdf.

B. The National Defense Authorization Act for Fiscal Year 2019 contains several important provisions focused on risks to the supply chain

On the same day that the Mitre report was released – 13 August 2018 – the president signed the National Defense Authorization Act (NDAA) for Fiscal Year 2019 into law. The act included several provisions that address the supply chain. The provisions focus on addressing risks in the supply chain that relate to cybersecurity and/or other risks that could compromise products, services, and systems used by the U.S. government.

Section 881. Permanent Supply Chain Risk Management Authority [10 U.S.C. §2339a].

The Secretary of Defense and the Secretaries of the Army, Navy, and Air Force, are given authority to exclude certain sources of supply in order to reduce supply chain risk. Supply chain risk is defined as the risk that an adversary may sabotage or subvert a covered system so as to "surveil, deny, disrupt or otherwise degrade the function, use or operation" of the system. This provision also provides authority to limit disclosure of information relating to any such exclusion. This authority may only be exercised after several steps have been taken related to the proposed exclusion, including the following: a joint recommendation must be obtained from the Under Secretary of Defense for Acquisition and Sustainment and from the DoD's Chief Information Officer that supports the planned exclusion based on a risk assessment by the Under Secretary of Defense for Intelligence. Further, there must be a finding that indicates that the action is necessary and there are no other less intrusive options available. In a case where disclosure of the basis for the action is to be withheld, the Secretary concerned must find the risk to national security of the disclosure outweighs the risks associated with not disclosing the information. Finally, notice must be given to the appropriate congressional committees. Of note, such exclusions are not reviewable in a bid protest before the Government Accountability Office (GAO) or in federal court. This provision is very similar to Section 806 of the NDAA for 2011, which contained a sunset provision of 30 September. Only the sunset provision itself has been repealed.

Section 889. Prohibition on certain telecommunications and video surveillance services or equipment.

This NDAA provision prohibits federal agencies from procuring equipment, systems, or services that use in pertinent part certain covered telecommunications equipment and services. The covered telecommunications equipment affected include telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation and its affiliates, as well as video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company and their affiliates, when used for public safety, security of government facilities, critical infrastructure, or other national security purposes. It also affects telecommunications or video surveillance services provided by these entities or by other entities using such equipment.

This provision also permits the Secretary of Defense to add suppliers to this list that it reasonably believes to be owned, controlled, or otherwise connected to a covered foreign country (defined in this Section 889 as the People's Republic of China). Such additions will be based on consultation with the Director of National Intelligence and/or of the Federal Bureau of Investigation. The prohibition against federal agencies' direct procurement of applicable equipment, systems, or services will take effect one year after the date of enactment of the 2019 NDAA. Although there is no mechanism for enlarging the definition of "covered foreign country" beyond China, Section 1654 of the NDAA requires the Secretary to prepare and maintain a list of "countries of concern" that pose a risk to the cybersecurity of the U.S., and to report that list to Congress. We expect that the list will inform congressional consideration of expanding the list of what is a "covered foreign country."

Section 1613. Evaluation and enhanced security of supply chain for protected satellite communications programs and overhead persistent infrared systems.

This section requires the Secretary of Defense to evaluate vulnerabilities in the DoD supply chain relating to each protected satellite communications and next generation overhead persistent infrared system by 31 December 2020. This evaluation is to be done in coordination with the Director of National Intelligence. The Secretary must, within 180 days of the enactment of the 2019 NDAA, brief congressional committees on its plan for completing these evaluations. The Secretary must also concurrently develop strategies and cost estimates associated with mitigating supply chain risks identified in this evaluation. Further, the Secretary is required to issue or revise a DoD instruction establishing the prioritization of supply chain risk management programs to ensure that acquisition and sustainment programs related to satellite communications and overhead persistent infrared systems receive priority.

Section 1644. Assistance for small manufacturers in the defense industrial supply chain and universities on matters relating to cybersecurity.

The Secretary of Defense, under this section of the 2019 NDAA, is required to take any actions that are needed in order to "enhance awareness of cybersecurity threats among small manufacturers and universities working on DoD programs and activities." The Secretary is expected to prioritize efforts required under this section, and must focus on such suppliers and universities that the Secretary considers critical. This section also requires mechanisms to be developed that will help small manufacturers and universities complete voluntary self-assessments with the support of various small business programs, and other engagements. These self-assessments are expected to help small businesses and universities understand "operating environments, cybersecurity requirements, and existing vulnerabilities." The Secretary is also required to promote the transfer, to small manufacturers and universities, of technology, threat information, and security techniques developed by the DoD. This effort is to be coordinated with other federal agencies, as appropriate. The Secretary is also required to establish or approve a certification program that will be used to train DoD staff to provide cyber planning assistance to small businesses and universities. Finally, the Secretary is authorized to take action to evaluate and improve cybersecurity resilience of the defense industrial base, if the Secretary determines it appropriate to do so.

Section 1655. Mitigation of risks to national security posed by providers of information technology products and services who have obligations to foreign governments.

Section 1655 requires that providers of products, services, or systems relating to information or operational technology, cybersecurity, an industrial control system, or weapons system, must disclose to the Secretary of Defense whether a foreign person and/or government has been allowed to review code of such products, services, or systems within five years prior to the enactment of the 2019 NDAA or anytime thereafter. Without such disclosures, DoD is prohibited from using such products, services, or systems that are acquired after the enactment of the 2019 NDAA. This provision of Section 1655 covers products, services, or systems developed for the DoD, and applies to any foreign government.

Another provision of section 1655 applies similar requirements to a far broader category of products, systems, or services if the disclosure is to a foreign government identified through Section 1654 as a country that poses a risk to the cybersecurity of the U.S. The section also obligates providers to disclose

where export licenses have been held or sought, for the export of IT products, components, software, or services that contain code developed for DoD. Upon receipt of disclosures, the Secretary of Defense will need to evaluate any risks to national security and must mitigate such risks, including by conditioning any agreement to use or procure the product, system, or service on the inclusion of enforceable requirements that would mitigate the risks. The Secretary must report on this to congressional committees on an annual basis. All disclosures collected from providers will be placed in a registry for future use in procurement actions, and may be exempted from disclosure under section 552 of Title 5, U.S.C. Additionally, within two years of the enactment of the 2019 NDAA, the Secretary must develop testing standards for commercial off the shelf (COTS) products, systems, or services, "to use when dealing with foreign governments."

Section 3117. Extension of enhanced procurement authority to manage supply chain risk.

This section extends the expiration date to 30 June 2023 of the existing authority granted to the Secretary of Energy, for enhanced procurement authority to manage supply risk (50 U.S.C. 2786). The authority granted includes authority to exclude sources and withhold consent to subcontract for covered systems and components which include national security systems, nuclear weapons, certain surveillance systems, and nonproliferation programs and systems. Such exclusions will be based on a failure to meet certain qualifications and other requirements that relate to supply chain risk.

Section 252. Improvement of the Air Force supply chain.

This section authorizes the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics to use up to US$42.8 million of the funds appropriated for research, development, test, and evaluation for nontraditional technologies and sustainment practices (such as additive manufacturing, artificial intelligence, predictive maintenance, and other software-intensive and software-defined capabilities) to improve availability of aircraft and parts, reduce supply chain risk, and to increase its ability to use additive manufacturing.

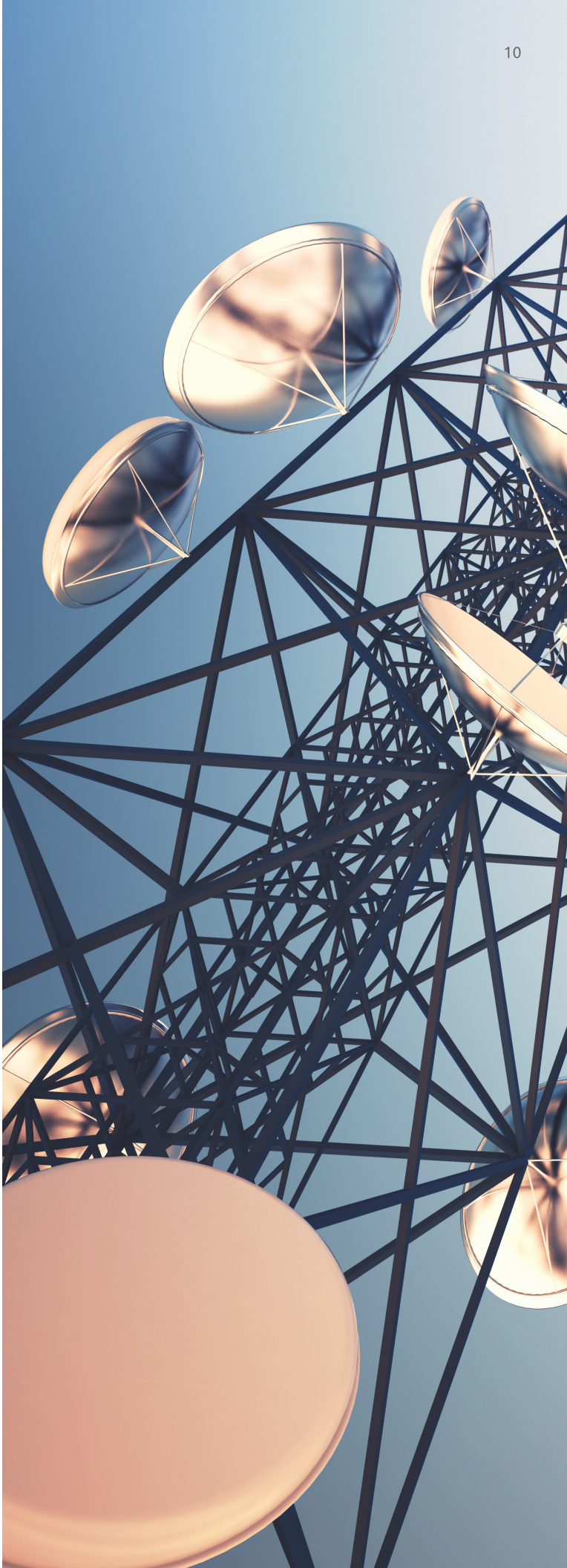
Section 871. Prohibition on acquisition of sensitive materials from non-allied foreign nations.

This NDAA provision prohibits, with certain limited exceptions, the Secretary of Defense from procuring or selling covered material to North Korea, China, Iran, and Russia. Covered material include samarium-cobalt magnets, neodymium-iron-boron magnets, tungsten metal powder, and tungsten heavy alloy.

C. Conclusion

As noted above, there is a need for a robust dialogue between the government and the contractor community about how to effectively address supply chain security risk without over burdening contractors (and, in turn, tax payers). In a later publication, we will set out some preliminary thoughts on select recommendations from the Mitre report.

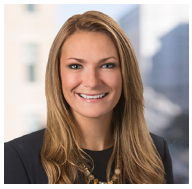
We hope to jump-start the robust dialogue between the government and contractors that is needed to better protect national security from malicious software and defective parts introduced into the supply chain, while preserving the huge benefits we obtain from the global supply chain we so depend on.



Authors and contacts

Michael Mason
Partner, ADG Industry Sector Lead
Washington, D.C.
T +1 202 637 5499
mike.mason@hoganlovells.com

Robert Taylor
Senior Counsel
Washington, D.C.
T +1 202 637 5657
bob.taylor@hoganlovells.com



Stacy Hadeka
Senior Associate
Washington, D.C.
T +1 202 637 3678
stacy.hadeka@hoganlovells.com

Michael Scheimer
Senior Associate
Washington, D.C.
T +1 202 637 6584
michael.scheimer@hoganlovells.com

William Kirkwood
Associate
Washington, D.C.
T +1 202 637 3675
william.kirkwood@hoganlovells.com

Rebecca Umhofer
Professional Support Lawyer
Washington, D.C.
T +1 202 637 6939
rebecca.umhofer@hoganlovells.com

Hogan Lovells

Aerospace, Defense, and Government Services Industry

We can help you anticipate and deal with the risks before they become problems.

The aerospace, defense, and government services (ADG) industry is changing significantly. Global spending on defense and weapon system platforms is increasing. Governments are procuring analysis and engineering services to address escalating terrorism threats, cybersecurity concerns, and an ever-increasing demand for big data analytics. Commercial space and unmanned vehicle advances have invigorated key sections of the industry. Brexit and the administration change in the U.S. are creating challenges and opportunities across the globe. And, technological advances such as 3-D printing are creating unique opportunities for innovative products, decreased time-to-market schedules, and agile maintenance and repair services.

Our clients demand experience. They need comprehensive and cost-effective support from lawyers who know their business and understand the demands of their industry.

That's where we come in.

Be ready

Our global ADG practice is focused specifically on your needs. Our team includes industry-leading lawyers with corporate, commercial, regulatory, investigations, and litigation experience. We work closely with some of the largest and most established ADG companies in the United States, Europe, and Asia. We advise dozens of middle market businesses, emerging companies, new ventures, global entities, along with investment banks and private equity firms that are active in the industry.

We know, because we've been there

Our clients are also some of the most innovative in the world. They build manned and unmanned aircraft, supply parts, and materials to the aerospace industry, and develop and deliver the technologies essential to defense and national security. Our clients make and provide launch vehicle and satellite services and provide the services and innovations required for homeland security and critical governmental operations.

So let's work together

Together we will tackle the difficult challenges, capitalizing on opportunities, and avoiding pitfalls. We will guide you through government regulatory and procurement hazards and protect your interests in disputes and government investigations. Our industry focus enables us to fully understand your business and the challenges you face. We anticipate emerging issues before they become a problem and we give advice that achieves results.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com