Morgan Lewis

REPORT

SMARTPHONES ON WHEELS

COMMERCE PROPOSES REGULATIONS TO ADDRESS NATIONAL SECURITY RISK FROM CONNECTED VEHICLES

OCTOBER 2024

SMARTPHONES ON WHEELS: COMMERCE PROPOSES REGULATIONS TO ADDRESS NATIONAL SECURITY RISK FROM CONNECTED VEHICLES

On September 23, 2024, the US Department of Commerce's Bureau of Industry and Security (BIS) published a notice of proposed rulemaking (NPRM) outlining new proposed rules to address national security risks associated with information and communications technology and services (ICTS) integral to connected vehicles that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign countries.

This rulemaking highlights the US government's concerns that user data collected by connected vehicles—including but not limited to sensitive data such as geolocation—could be exploited by certain countries for national security gain, similar to how smartphones and other connected devices are potential intelligence targets.

The NPRM follows BIS's March 2024 advanced notice of proposed rulemaking (ANPRM) issued under Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain." The ANPRM received 57 comments from original equipment manufacturers (OEMs), component suppliers, foreign governments, nonprofit organizations, and individuals. After BIS reviews additional comments submitted in response to the new NPRM, we expect BIS to finalize the rules, which will take effect 60 days after publication of the final rules in the *Federal Register*. The NPRM builds on the ANPRM, which we previously summarized in a March 2024 Insight and LawFlash.

The draft rules were published in the *Federal Register* on September 26, 2024, with the comment period closing on October 26, 2024 (however, since October 26 falls on a Saturday, comments can actually be submitted until the following Monday, October 28, 2024).

In this report we summarize some of the main elements of the NPRM as well as analyze the key implications for various stakeholders.

SCOPE AND KEY DEFINITIONS

The draft rules identify significant cybersecurity and national security risks in the connected vehicle supply chain due to certain foreign countries' ability to access sensitive data or introduce vulnerabilities into US infrastructure. These concerns are particularly acute given the integration of Vehicle Connectivity Systems (VCS) and Automated Driving Systems (ADS) in modern vehicles, and as such the proposed rules target VCS and ADS that are designed, developed, manufactured, or supplied by persons owned or controlled by certain foreign countries, currently scoped to include the People's Republic of China (PRC or China) and Russia.

It is notable that although BIS previously identified six systems (i.e., vehicle operating systems (OS), telematics systems, Advanced Driver-Assistance System (ADAS), Automated Driving Systems (ADS), satellite or cellular telecommunications systems, and battery management systems (BMS)) in the ANPRM, based on public comments BIS ultimately chose to subject only VCS and ADS to the proposed regulations, explaining that this deliberate choice was being made to strike a balance between minimizing supply chain disruptions and addressing the national security risks by focusing on those systems that most directly facilitate the transmission of data both to and from the vehicle, rather than focusing on all systems.

Important definitions include the following:

Connected software is defined to mean the software-based components, in which there is a foreign interest, executed by the primary processing unit of the respective systems that are part of an item that supports the function of VCS or ADS at the vehicle level. Notably, this definition excludes firmware, which refers to software designed specifically to control, configure, and communicate with hardware devices. It also does not cover open-source software that is freely accessible, modifiable, and distributable by anyone, provided both the source code is available and contributions to its development are permitted. However, if open-source software has been modified for proprietary use and not redistributed or shared, it would be considered covered software.

Connected vehicles is defined to mean "[a] vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways[] that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Vehicles operated only on a rail line are not included in this definition." According to the proposed rules, this definition captures, for example, passenger vehicles, motorcycles, buses, small and medium trucks, class 8 commercial trucks, recreational vehicles, and unmanned aerial vehicles.

Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary generally includes (1) anyone acting under the order, request, or control of a foreign adversary or someone whose activities are directed or financed by a foreign adversary; (2) any citizen or resident of a foreign adversary nation who is not a US citizen or permanent resident; (3) any organization headquartered, incorporated, or operating under the laws of a foreign adversary; and (4) any organization controlled by a foreign adversary, including cases where control is exerted through ownership, voting power, board representation, or formal/informal arrangements.

Vehicle connectivity systems (VCS) is defined to mean hardware or software items for a completed connected vehicle that has the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz. This definition would exempt most remote keyless entry fobs and immobilizers and certain internal wireless sensors and relays. This definition will, however, encompass hardware and software systems—such as the telematics control unit (TCU), cellular modems and antennas, and other automotive components—that integrate various radio frequency communication technologies and enable connected vehicles to access external data sources, facilitate vehicle-to-vehicle communication, and provide enhanced services to users through seamless connectivity options.

VCS hardware, relatedly, is defined to mean software-enabled or programmable components and subcomponents that support the function of VCS or are part of an item that supports the function of VCS: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or modules, Bluetooth microcontrollers or modules, satellite navigation systems, satellite communication systems, other wireless communication microcontrollers or modules, and external antennas.

Automated driving systems (ADS) is defined to mean hardware and software that, collectively, are capable of performing the entire dynamic driving task for a completed connected vehicle on a sustained basis, regardless of whether it is limited to a specific operational design domain. BIS notes that this definition is consistent with the SAE J3016 standard, which defines autonomy levels ranging from Level 0 (no automation), where the driver controls all aspects of driving, to Level 5 (full automation), where the vehicle can operate independently under all conditions without human intervention. For purposes of the

final rules, BIS specifically defines ADS to correspond to automation levels 3, 4, and 5. The terms VCS and ADS are collectively referred to as "Covered Software" in the proposed rules.

Owned by, controlled by, or under the direction of a foreign adversary is defined to generally cover (1) individuals acting on behalf of a foreign adversary or those controlled, financed, or directed by one; (2) citizens or residents of a foreign adversary's country who are not US citizens or permanent residents; (3) organizations headquartered or incorporated in a foreign adversary's country; and (4) organizations owned or controlled by a foreign adversary, where control can be exerted through ownership, voting rights, board representation, or other means to influence decision-making.

- Compared with the definition proposed in the ANPRM, this version notably excludes US citizens and permanent residents who are also residents of a foreign adversary. It clarifies that an entity's location is determined by its principal place of business, headquarters, or place of incorporation. Additionally, it expands coverage to include indirect control through various mechanisms such as ownership of a majority or dominant minority of voting interests, board representation, proxy voting, special shares, contractual arrangements, or other formal or informal agreements to act in concert.

- Moreover, unlike for example the definition of a Foreign Entity of Concern (FEOC) under the Inflation Reduction Act, under which a subsidiary is not automatically deemed an FEOC unless it independently meets the subject-to-jurisdiction or ownership criteria, the proposed rules here do not set a specific 25% threshold for voting rights, equity shares, or board seats under the definition of "owed by, controlled by, or under the direction of a foreign adversary."

Foreign interest is defined to cover, when used with respect to property, any interest in property, of any nature whatsoever whether direct or indirect, by a non-US person. Under this definition, a foreign interest can include but is not limited to an interest through ownership, intellectual property, contract—e.g., ongoing supply commitments such as maintenance, any license agreement related to the use of intellectual property—profit-sharing, or fee arrangement, as well as any other cognizable interest.

To provide clarity regarding "ownership," "control," and "under the direction," the NPRM also sets out examples, and seeks comments on whether the guidance and examples are sufficiently clear:

Example	Scenario Summary	Ownership/Control/Direction
Example 1	Company A, incorporated in the US, is a wholly owned subsidiary of Company B, a state-owned enterprise from the PRC or Russia.	Because of Company B's ownership structure as a state-owned entity, Company A is considered to be directly "owned by" the PRC or Russia, even though it is incorporated in the US.
Example 2	Company A is a joint venture between Company B and Company C. While Company B is incorporated in a third-party jurisdiction, Company C, which holds the majority stake, is a state-owned enterprise from the PRC or Russia.	Due to Company C's majority control, Company A is considered to be "owned by" the PRC or Russia.
Example 3	Company A is majority-owned by a group of state-owned enterprises and state-owned investment funds from the PRC or Russia.	The collective ownership by these PRC or Russian state-owned entities means that Company A is considered to be "owned by" the PRC or Russia.

Example 4	Company A, incorporated in the US, is a subsidiary of Company B, a private company headquartered in the PRC or Russia. Although Company B is private, its principal place of business in the PRC or Russia means it is under their jurisdiction.	Company A is "controlled by" and "subject to the direction of" the PRC or Russia.
Example 5	Company A is a multinational corporation where the majority of voting power is held by Company B, an investment fund controlled by the PRC or Russian government.	Despite the multinational status of Company A, it is "controlled by" the state-owned fund and makes Company A "subject to the direction of" the PRC or Russia.
Example 6	Company A, a holding company with a complex dual-class share structure, is publicly listed. Class B shares have 10 times the voting power of Class A shares.	If the aggregate voting power of PRC or Russian shareholders, across both classes, forms a majority or dominant minority, Company A would be considered as "controlled by" and "subject to the direction of" PRC or Russia.
Example 7	Company A, based in the PRC or Russia, holds a minority interest in Company B, a US business. Despite the minority share, Company A has special veto rights over major decisions at Company B, including the power to veto executive dismissals, thus effectively controlling Company B.	Company B is "controlled by" and "subject to the direction of" the PRC or Russia.
Example 8	Company A, incorporated in a third country, forms a joint venture (Company C) with Company B (PRC or Russian), and Company D (a PRC citizen-owned holding company) holds the largest minority share.	If the combined voting power of Company B and Company D constitutes a majority or dominant minority, Company C would be considered "controlled by" and "subject to the direction of" PRC or Russia.
Example 9	Company A has a corporate governance structure requiring a 75% supermajority vote for major decisions. Three of the eight board members are from the PRC or Russia, and their 37.5% voting power gives them the ability to block any significant decisions, thus giving them effective control over Company A.	Company A is "controlled by" or "subject to the direction of" the PRC or Russia.
Example 10	The PRC or Russian government, through an investment fund, acquires a 1% special management share in Company A. This share gives the government the right to appoint a director to the board and veto major decisions such as mergers or strategic changes, allowing	Company A is "controlled by" the PRC or Russia.

	significant influence over Company A's operations.	
Example 11	Company A maintains its principal place of business in the PRC or Russia, making it subject to the legal jurisdiction of those countries.	Company A is "subject to the jurisdiction of" the PRC or Russia.
Example 12	Company A, a US-based publicly listed entity, has a wholly owned subsidiary, Company B, which is incorporated and operates in the PRC or Russia. Although Company B is subject to PRC or Russian jurisdiction, Company A itself is not considered under their jurisdiction simply because of its subsidiary's location.	Company B is "subject to the jurisdiction of" the PRC or Russia, but Company A is not.
Example 13	Company A, a US private company, has a board member (Person X) with close ties to the PRC government, **including past roles at PRC corporations and investment facilitation**. Due to Person X's ownership stake, influence over the CEO, and government ties, Company A is considered subject to the direction of the PRC.	Company A is "subject to the direction of" the PRC.

PROHIBITIONS

The proposed rules would, absent a general or specific authorization (discussed below):

1. Prohibit VCS hardware importers from knowingly importing into the United States certain VCS hardware designed, developed, manufactured, or supplied by persons owned, controlled by, or subject to the jurisdiction of China or Russia;

2. Prohibit connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating certain software that supports the function of Covered Software designed, developed, manufactured, or supplied by persons owned, controlled by, or subject to the jurisdiction of China or Russia;

3. Prohibit connected vehicle manufacturers from knowingly selling within the United States completed connected vehicles that incorporate Covered Software; and

4. Prohibit connected vehicle manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or Covered Software.

The NPRM provides the following examples to further illustrate the sort of transactions involving VCS hardware and Covered Software that would be prohibited:

Example	Scenario Summary	Prohibited?
Example 14	A US company imports a cellular module manufactured at a PRC or Russian facility and routed through a third country. Since the manufacturer is under PRC or Russian jurisdiction, the import of the module would be prohibited unless authorized by BIS.	Prohibited import unless authorized by BIS.
Example 15	A US company imports a telematics control unit (TCU) assembled in a third country that contains a microcontroller made in the PRC or Russia. The TCU is classified as VCS hardware, making its import prohibited unless authorized by BIS.	Prohibited import unless authorized by BIS.
Example 16	A US company imports a connected vehicle containing software for off-vehicle connectivity, which was designed or developed by a PRC or Russian entity. The vehicle import would be prohibited unless authorized by BIS.	Prohibited import unless authorized by BIS.
Example 17	A US manufacturer sells a connected vehicle that contains proprietary software designed by a PRC or Russian entity for automated driving systems. This sale would be prohibited under the rule unless authorized by BIS.	Prohibited sale unless authorized by BIS.
Example 18	A US connected vehicle manufacturer uses PRC or Russian-based software development teams for VCS and ADS software. Given the involvement of PRC or Russian entities, the sale of the vehicle within the US would be prohibited unless authorized by BIS.	Prohibited sale unless authorized by BIS.
Example 19	A US connected vehicle manufacturer uses software development teams that include PRC or Russian citizens, but these individuals work in a foreign jurisdiction for non-PRC or Russian companies. The fact that PRC or Russian citizens are involved does not automatically make the vehicle sale prohibited.	The sale is not prohibited under the rule.
Example 20	Company A, a subsidiary of a foreign corporation with PRC or Russian ownership, imports connected vehicles with VCS hardware and software. Although Company A did not design the software, it has access to the technology, and any subsequent sale would be prohibited without BIS authorization.	Prohibited sale unless authorized by BIS.
Example 21	Company A, a US-based manufacturer controlled by a PRC or Russian entity, sells vehicles with VCS hardware and software supplied by non-PRC or Russian companies. However, because Company A is controlled by the PRC or Russia and participated in the design of the technology, the sale is prohibited without BIS authorization.	Prohibited sale unless authorized by BIS.

Examples 20 and 21 underscore the United States' heightened national security concerns. Even when the development and manufacturing of hardware, software, or complete vehicles do not directly involve PRC or Russia, any involvement of companies controlled by the PRC or Russia in the supply chain—whether through access to or design by these components—is still considered a national security risk. In other words, the national security concern is not just about direct involvement from "adversarial" countries, but

extends to any level of indirect influence or control by companies based in or controlled by such countries.

COMPLIANCE MECHANISMS

In the ANPRM, commenters referenced many best practices and standards, including the National Highway Traffic Safety Administration's Cybersecurity Best Practices for the Safety of Modern Vehicles, the International Organization for Standardization's and SAE International's standard ISO/SAE 21434, the Institute of Electrical and Electronics Engineers Standards Association's standard IEEE 1609.2, SAE J3061, and SAE J3161, as well as the United Nations Economic Commission for Europe's Regulations 155 (R155) and R156 on the international level.

BIS, however, has chosen not to incorporate cybersecurity standards and best practices into the rule, explaining that such measures alone are inadequate to mitigate supply chain risks because these systems cannot be fully protected against threats from OEMs or tier 1 and 2 suppliers that hold or maintain privileged access to them.

Instead, BIS proposes to adopt mechanisms for manufacturers to request authorizations or exemptions from BIS, including the possibility of demonstrating mitigation of security risks through certain compliance measures, including the following:

Declarations of Conformity, submitted to BIS by VCS hardware importers and connected vehicle importers and manufacturers to confirm that they are not engaging in prohibited transactions involving VCS hardware or covered software, as defined.

- Under the proposed rules, declarants would be responsible for submitting information to BIS, including documentation collected from suppliers of components of VCS hardware and from suppliers of covered software, to verify compliance with the regulations.
- These requirements include obtaining and analyzing the Hardware Bills of Material (HBOMs) for VCS hardware and the Software Bills of Material (SBOMs) for covered software and providing documentation of the steps the declarant took to verify that the transactions comply with the provisions of the rule. The proposed rules also explain in greater detail the types of Declarations of Conformity, which include the information required for VCS hardware importers (which will require an FCC ID number and HBOM) and completed connected vehicle manufacturers (which will require an SBOM that contains the author's name, timestamp, supplier name, component name, component hash, URL, dependency relationships, etc.)
- The Declaration of Conformity must be submitted to BIS annually, 60 days prior to the first sale of first import of a VIN series of completed connected vehicles comprised of a single year, or 60 days prior to the import of VCS hardware to certify that the submitter has not engaged in a prohibited transaction and provide certain information on the import of VCS hardware and/or the import or sale of completed connected vehicles.

General Authorizations, to allow certain VCS hardware importers and connected vehicle manufacturers to engage in otherwise prohibited transactions without the need to notify BIS prior to the prohibited activity if they qualify under a narrow set of circumstances.

- BIS proposes that VCS hardware importers and connected vehicles manufacturers may self-certify one or more of four proposed general authorizations: (1) the connected vehicle manufacturer or VCS hardware importer and entities under common control, including parents, engaging in an otherwise prohibited transaction produces a total model year production of

completed connected vehicles containing covered software or total model year production of VCS hardware that is less than 1,000 units; (2) the completed connected vehicle that incorporates the VCS hardware or covered software is on public roadways fewer than 30 calendars days in any calendar year; (3) the completed connected vehicle would only be used for display, testing, or research and not be on public roadways; or (4) the completed connected vehicle is imported only for repair, alteration, or competition off public roads and will be reexported within a year of import.

- Entities using general authorizations must self-certify compliance, maintain records for 10 years, and monitor for changes that would make them ineligible. If no longer eligible, specific authorization must be sought. However, subsidiaries or entities controlled by the PRC or Russia are ineligible for general authorizations and must apply for specific authorizations.

Advisory Opinions, to allow VCS hardware importers and connected vehicle manufacturers to seek guidance from BIS on whether a prospective transaction may be prohibited.

- A request for an advisory opinion must contain contact information for the submitter as well as all current information on the prospective transaction to assist BIS in making a determination.
- Additional information would include technical details on the involved VCS hardware or covered software, information on the completed connected vehicle (if applicable), the SBOM and/or HBOM for the covered software and/or VCS hardware, and any other supporting materials that the submitter assesses will assist BIS in determining if the transaction may be prohibited by this rule.

Specific Authorizations, which, following an application to and approval by BIS (reviewed on a case-specific basis), grant VCS hardware importers and connected vehicle manufacturers the ability to engage in otherwise prohibited transactions, including because the associated undue or unacceptable risks have been, or can be, mitigated.

- When reviewing applications for specific authorization, BIS will evaluate factors that may pose undue or unacceptable risks, particularly concerning the potential exfiltration of data or remote manipulation of connected vehicles. Key considerations include the applicant's ability to limit PRC or Russian government access or influence over the VCS hardware or software, the security standards in place (and whether they can be validated by BIS or a third party), and any mitigation measures proposed by the applicant to reduce risks.
- The time to reach a decision on an application for a specific authorization will vary based on the complexity of the case. However, BIS will respond to applicants with a processing update within 90 days of the initial application for a specific authorization, and typically endeavor to provide either a request for more information or a decision within that period.
- As a condition of approving the specific authorization, BIS might impose certain requirements and mitigation measures upon the VCS hardware importers and connected vehicles manufacturers seeking to proceed with the prohibited transaction.

"Is-Informed" Notices, which allow BIS to inform VCS hardware importers or connected vehicle manufacturers, via direct letters or a *Federal Register* notice, that a specific transaction involving certain software, hardware, or entities requires a specific authorization due to it being classified as a prohibited transaction. If a party proceeds with the transaction after receiving an "is-informed" notice without obtaining the required authorization, it would be in violation of the rule.

BIS also proposes to create a mechanism by which any person whose application for a specific authorization is denied, whose specific authorization is suspended or revoked, or who has received a written notification of ineligibility for a general authorization may appeal that decision to the Under Secretary. Additionally, violators would be subject to civil and criminal penalties according to the International Emergency Economic Powers Act.

EXEMPTIONS AND COMPLIANCE TIMELINE

Manufacturers and importers would be given time to come into compliance, with deadlines set for the 2027 model year for software and the 2030 model year for hardware. Exemptions exist for vehicles produced prior to these deadlines. Specifically, VCS hardware importers would be permitted to engage in otherwise prohibited transactions involving VCS hardware and exempt from certain requirements so long as:

- For VCS hardware not associated with a model year, the import of the VCS hardware takes place prior to January 1, 2029; or
- The VCS hardware unit is associated with a vehicle model year prior to 2030 or the VCS hardware is integrated into a connected vehicle (completed or incomplete) with a model year prior to 2030.
- Connected vehicle manufacturers would be permitted to engage in otherwise prohibited transactions involving covered software and exempt from certain requirements so long as the completed connected vehicle that is imported, or sold within the United States, is of a model year prior to 2027.
- Connected vehicle manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would be permitted to sell completed connected vehicles with a model year prior to 2027 that incorporate VCS hardware or covered software.

KEY IMPLICATIONS

As the United States pushes for greater transparency in supply chains and increased domestic production, the proposed rules introduce several key effects for connected vehicle companies regardless of whether they are based in the United States or internationally. Evidently, major vehicle manufacturers that have been reliant on Chinese or Russian technology may face considerable challenges as a result of increased scrutiny from regulatory authorities.

To ensure they do not inadvertently engage in prohibited transactions, these companies will likely need to overhaul their compliance systems, conducting deep supplier audits with a specific focus on VCS and ADS. This could also mean rethinking sourcing strategies, especially for key components such as connectivity and ADS systems. Suppliers of microcontrollers, software, sensors, and telecommunications equipment that incorporate such technology will need to diversify their sourcing or invest in developing alternative technologies, all of which could significantly reshape their supply chain.

In response to these restrictions, Chinese companies involved in the connected vehicle industry may also look to restructure or otherwise modify their operations to navigate these new barriers. This restructuring could involve, for example, establishing subsidiaries or joint ventures in other countries with modified ownership and operational structures that are not subject to the ownership, control, or direction of certain other foreign countries.

This rule is part of a broader effort under Executive Order 13873, which aims to secure the US technological infrastructure by reducing reliance on suppliers from countries of concern. Commerce previously promulgated rules to implement the executive order and regulate more traditional types of ICTS but is now expanding its use of the executive order to cover connected vehicles as well. It is possible this expansion could also set the stage for future regulations under Executive Order 13873 covering other high-risk technologies beyond connected vehicles, such as unmanned aerial vehicles or other types of components such as LiDar.

The proposed rules also reflect the US government's ongoing concern about the ways in which sensitive data of US persons can potentially be leveraged by an adversary for national security gain. In this way, the Commerce NPRM is consistent with other efforts by the US government to protect sensitive data through other national security regulatory processes including the Committee on Foreign Investment in the United States (CFIUS), the Committee for the Assessment of Foreign Participation in the United States Telecommunications Service Sector (more commonly known as Team Telecom), and a pending rulemaking by the US Department of Justice's Foreign Investment Review Section pursuant to Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern."

As companies across various sectors look at the increasing regulatory efforts to protect consumer data for national security reasons, they may view such measures as a market signal that the US government is sending to reduce reliance on suppliers from countries deemed adversarial and to begin shifting parts of their production back to the United States or allied nations. This trend could lead to long-term shifts in global supply chains as businesses aim to mitigate the risk of future regulatory challenges.

With respect specifically to Commerce's proposed rules for connected vehicles, affected companies are likely to react in various ways. Some may rely on the ability to seek specific licenses or may seek modifications to the rules by submitting comments to the NPRM. Others may opt for advisory opinions or rely on general authorizations to ensure their operations comply with the new regulations while maintaining business continuity. These legal and regulatory maneuvers will be critical for companies aiming to navigate the complexities of the rule while preserving their competitive advantage in the market.

HOW WE CAN HELP

Our team has a command of the full spectrum of issues that our clients face in the industry, including one of our lawyers, David Plotinsky, who was the original drafter of Executive Order 13873, which is the legal basis for the Commerce NPRM discussed in this report.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Boston

Daniel S. Savrin	+1.617.951.8674	daniel.savrin@morganlewis.com
Carl A. Valenstein	+1.617.341.7501	carl.valenstein@morganlewis.com

Philadelphia

Mark J. Fanelli	+1.215.963.5069	mark.fanelli@morganlewis.com

San Francisco

Brent A. Hawkins	+1.415.442.1449	brent.hawkins@morganlewis.com
Pejman Moshfegh	+1.415.442.1451	pejman.moshfegh@morganlewis.com

Shanghai

Todd Liao	+86.21.8022.8799	todd.liao@morganlewis.com

Washington, DC

Giovanna M. Cinelli	+1.202.739.5619	giovanna.cinelli@morganlewis.com
David Plotinsky	+1.202.739.5742	david.plotinsky@morganlewis.com
Ivon Guo	+1.202.739.5163	ivon.guo@morganlewis.com
R. Latane Montague	+1.202.739.5582	latane.montague@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.

Morgan Lewis

At Morgan Lewis, we're always ready to respond to the needs of our clients and craft powerful solutions for them.

Connect with us

www.morganlewis.com

100424_241978