Morgan Lewis

TECHNOLOGY MAY-RATHON

Hot Topics in Supply Chain Cybersecurity

Presenters

Dan Skees

Bobby Goldfin

Arjun Ramadevanahalli

Morgan Lewis

Agenda

- Supply Chain Risks for Industrial and Critical Infrastructure
- New Federal Initiatives
- Mitigating Supply Chain Risks
- Commercial Considerations
  - Getting to "Yes" with Your Vendor
  - Assessing Supply Chain Risks During a Deal
  - Managing Liability

Risks for Industrial and Critical Infrastructure

Morgan Lewis

It takes 20 years to build a reputation and [a] few minutes of cyber-incident to ruin it.

- Stephane Nappo

The Threat to Industrial and Critical Infrastructure Is Different

- Damages are **not strictly direct financial harm** to the affected corporation
- February 2021 Oldsmar water treatment facility hack
  - Dangerous increase sodium hydroxide concentration
- August 2017 TRISIS incident (Saudi petrochemical facility hack)
  - Rare shutdown of industrial safety control systems
- August 2003 Northeast Blackout: approximately $6 billion in total economic cost
  - Shut down of 70 auto plants, idling 100,000 workers
  - Steel, chemical, refinery plants knocked offline
  - New York City suffered $1 billion in economic cost, including $250 million in frozen and perishable food

The Threat to Industrial and Critical Infrastructure Is Different

- Public health concerns
  - Sewage contamination and resulting public health problems
  - Property losses (accidents, crime)
- Costs to state and local government
  - Overtime costs for first responders
  - Lost tax revenue due to drop in economic activity
  - Increased litigation, including insurance recovery issues
- Impact of COVID-19 pandemic
  - Remote working posture and strained resources increases risks (more targets)

SolarWinds Supply Chain Breach

- 2020 Substantial breach of Orion software supply chain
  - Exploit allowed malicious actors to gain access to widely used network traffic management systems
- Estimated 18,000 downloads of the affected update
- Alarming scope of affected federal agency information systems
- NERC: 25% of electric utilities in the US and Canada downloaded SolarWinds backdoor

2021 Florida Water System Attack

- Hacker gained remote access to Oldsmar, Florida water treatment control system, increasing the amount of lye added to the water
  - Lye used in small amounts to control acidity, but larger amounts could be dangerous
  - Hacker changed it from 100 parts per million to 11,100 parts per million
- Caught by worker on duty who noticed the change and immediately corrected it

"The Oldsmar water treatment facility hack was entirely avoidable – and it can happen again"

2021 Colonial Pipeline Incident

- Largest U.S. pipeline system for refined oil products
- Caused by ransomware attack on company computer systems
- Unknown IT/OT access; facts developing
  - Disconnected OT systems to silo ransomwhere in IT environment
- Effects:
  - Scattered gas shortages across the southeastern US
  - Gas price spikes
  - State of emergency declared by governors in multiple states
- Colonial paid $4.4 million to attackers

Fines and Legal Liability

- Regulatory fines
  - Electric/NERC Reliability Standards: Statutory maximum is $1 million, per day, per violation, but costs add up in other ways as well
- Tort claims
- SEC/securities disclosure
- Data privacy laws (California, Virginia)


New Federal Initiatives
Morgan Lewis

Executive Order 14017
Securing America's Critical Supply Chains

- February 2021 – President Biden signs Executive Order addressing vulnerabilities in the supply chains of critical national economic sectors
  - Protection of key industrial sectors from supply chain shocks and vulnerabilities, including sectors implicated in the administration's focus on combatting climate change
- Two main components
  1. 100-day review of supply chain risks impacting four key product categories:
     - semiconductors
     - critical minerals, like rare earth elements
     - pharmaceuticals
     - "high capacity" batteries, including electric vehicle batteries
  2. Long-term review of supply chains
     - defense industrial base
     - the public health and biological preparedness industrial base
     - information and communications technology (ICT) industrial base
     - supply chains for agricultural commodities and food production
     - transportation industrial base; and energy sector industrial base

DOE 100 Day Plan

- DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and electric utilities to advance technologies to shore up electric industrial control systems
  - Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities;
  - Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks;
  - Reinforces and enhances the cybersecurity posture of critical infrastructure information technology (IT) networks; and
  - Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.

*Source: US Department of Energy

Executive Order 13920
Securing the United States Bulk-Power System

- May 1, 2020: President Trump signs Executive Order 13920
  - Imposed restrictions on transactions involving "bulk-power system equipment" provided by entities controlled by foreign adversaries where the transaction would create an undue risk
  - DOE directed to develop regulations by late-2020
- December 17, 2020: DOE issues the "Prohibition Order" limiting some utilities acquisitions or installations of certain bulk-power system equipment
  - Targeted select equipment "manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China"
- January 20, 2021: President Biden suspends EO 13920 for 90 days
- April 20, 2021: DOE revokes Prohibition order
- Currently: DOE collecting more comments from industry under an RFI

New Federal Cybersecurity Executive Order 14028
Executive Order on Improving the Nation's Cybersecurity

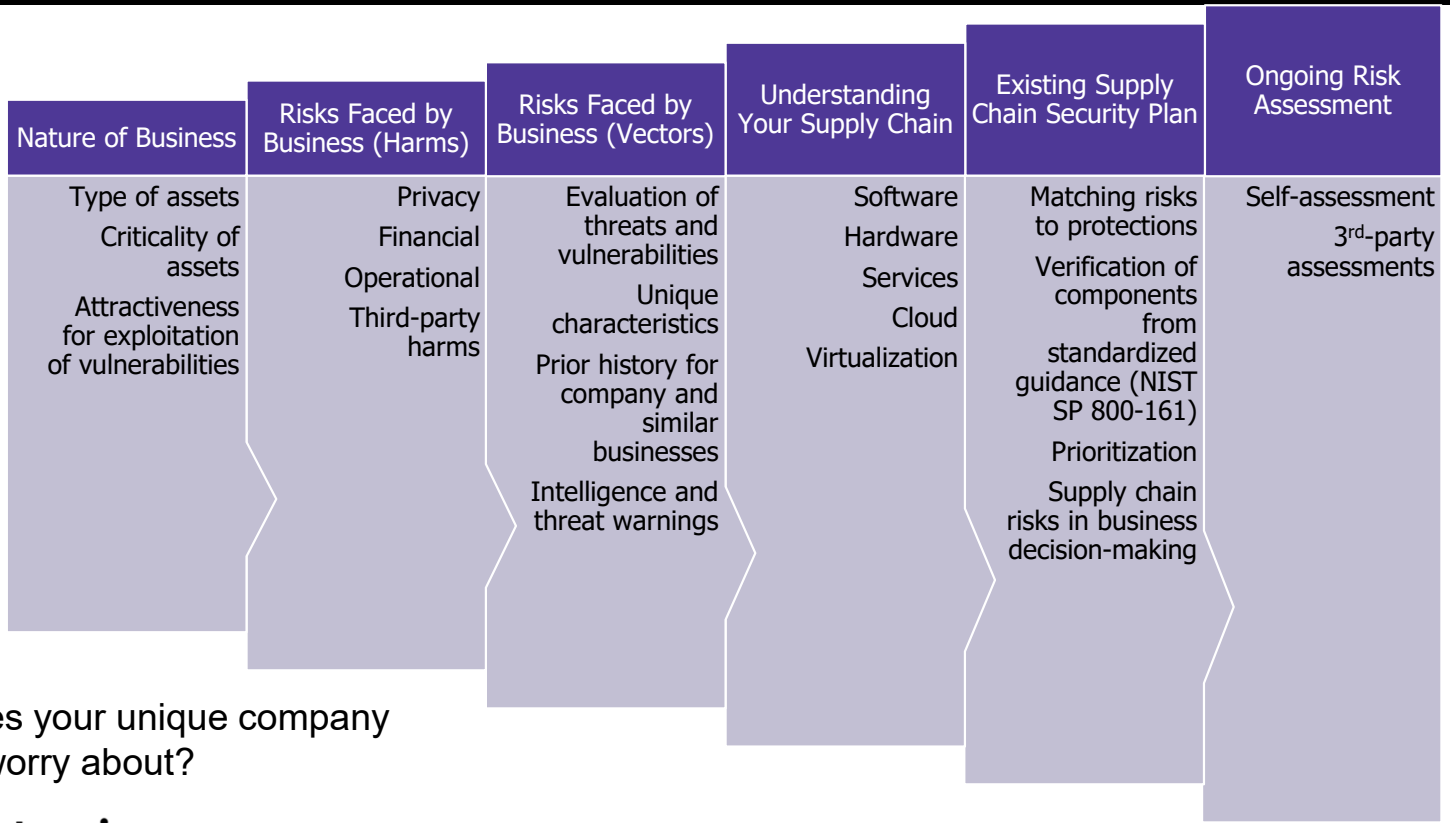
- Objective: Protect federal government networks and software supply chains against increasing threats of attacks from malicious actors and improve response capabilities
- Key features:
  - *Information Sharing:* Requires IT and communication government contractors to share information with agencies about cyber threats and to report cyber incidents
  - *Modernizing Cybersecurity*: Adoption of cloud networks and multifactor authentication
  - *Security Best Practices*: New security standards for software sold to the government to address vulnerabilities in software supply chains
  - *Cybersecurity Safety Review* Board: Co-chaired by government and private sector leads, to analyze significant cyber incidents and make recommendations.
  - *Cybersecurity incidient response*: Agency playbook and government-wide endpoint detection and response.
  - *Logging*: Cybersecurity event log requirements for federal departments and agencies.

Other Federal Initatives

- Interim National Security Strategy Guidance
- CISA and NIST interagency report "Defending Against Software Supply Chain Attacks"
- NIST publication NISTIR 8276 "Key Practices in Cyber Supply Chain Risk Management (C-SCRM): Observations from Industry"
- FCC Supply Chain Security Strategy


Identifying and Mitigating Supply Chain Risks
Morgan Lewis

Understand Your Unique Supply Chain Risks

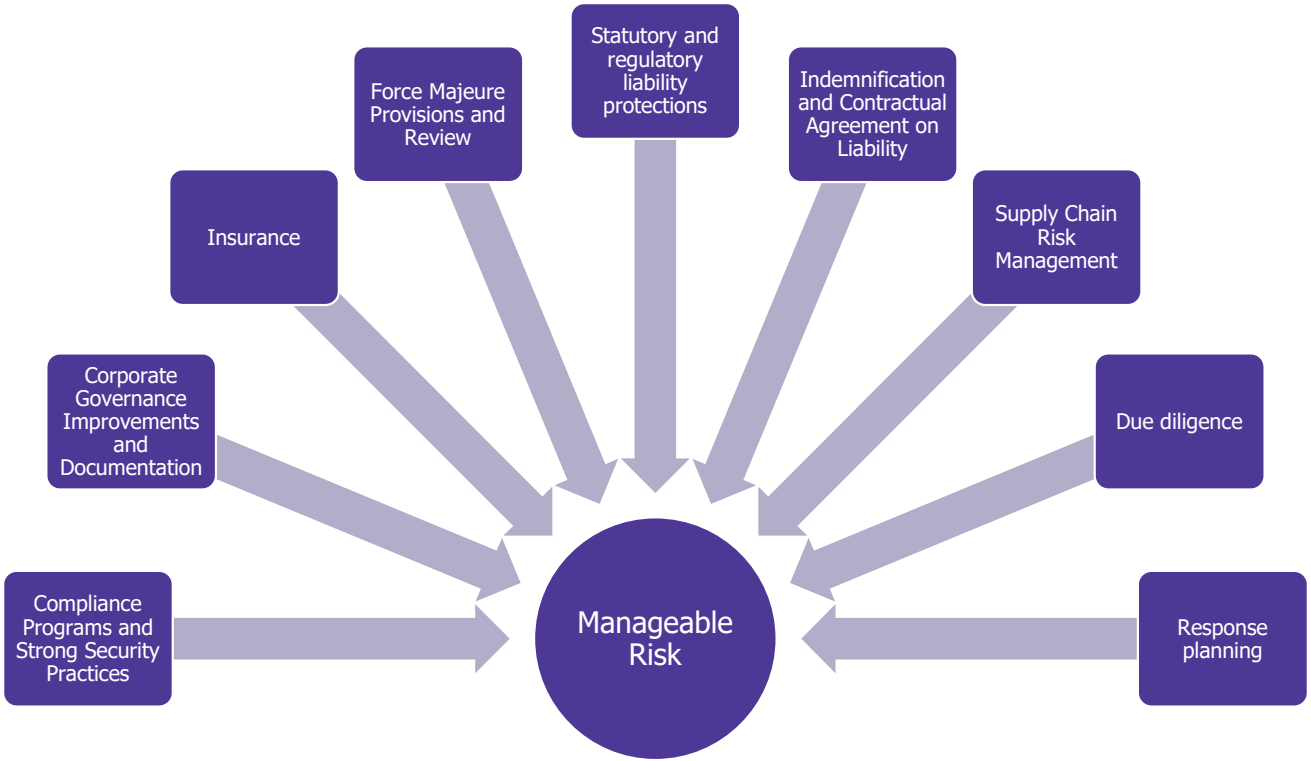


What does your unique company need to worry about?

Identifying Your Supply Chain Legal Liability

Consumer Protections	•State Notification Requirements (e.g., Tex. Bus. & Com. Code §§ 521.002, 521.053) •Federal Consumer Protection (e.g., Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1)) •Privacy Act requirements (e.g. California and Virginia)
Corporate Issues	•Securities Disclosures (SEC Corporation Finance Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011)) •Officer & Director Liability (*In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996))
Tort Liability under State Law	•Direct harms (loss of power, water, gas, telephone communications, etc.) •Indirect harms (widespread economic damages resulting from loss or misuse of critical infrastructure, *Pac. Bell v. So. Cal. Edison Co.* 208 Cal.App.4th 1400 (2012))
Contract Liability	•Security commitments in contracts with customers, vendors, counterparties •Confidentiality commitments
Mandatory Cybersecurity Obligations	•NERC Critical Infrastructure Protection Standards (18 CFR Part 39; 16 USC 824o) •Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards (48 CFR 204.73) •EO 14028 requirements for federal contractors

Legal Mechanisms to Manage Supply Chain Cyber Incident Liability Risks



Mitigating Supply Chain Risks (Internal Practices)

Morgan Lewis

Protect Yourself Through Good Cybersecurity Hygiene

- Apply NIST Cybersecurity Framework with a goal of achieving the appropriate target profile (making yourself a harder target)
  - Established as a result of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Feb. 2013) (V1.1 issued in April 2018)
- Measure cybersecurity policy against a standardized current cybersecurity guideline to avoid gaps
  - NIST Special Publication 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (Updated Jan. 2015)
  - Consider relevance of certifications (such as ISO/IEC 27001)
- Conduct audits of cybersecurity program compliance, including security tests, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks
  - Third-party reviews can be critical here, as they often bring a different perspective and review unexpected areas

Control What Is In Your Hands Regardless of Vendor Cooperation

- Significant portions of supply chain security concerns are best addressed in coordination with vendors and their suppliers, but even in the absence of that coordination, significant steps can be taken to reduce supply chain cybersecurity risk.

1. Track public alerts and databases of incidents related to vendors and vulnerabilities related to vendor-provided products and services
2. Develop an incident response plan for supply chain cyber incidents, which require a different approach
3. Track and grant vendor access to networks, physical locations, and sensitive information repositories based on need
   a) Review need decisions regularly and revoke quickly
   b) Limit access to narrow group of non-company personnel
4. Verify software integrity and authenticity
5. Establish strict controls for remote access and system-to-system communications by vendor
6. Coordinate with your ISAC or other governmental points of contact to remain informed on known risks
7. Enhance confidentiality arrangements with vendors
8. Use FOIA-exempt disclosure processes for governmental information-sharing programs
9. Review cyber insurance


Assessing Supply Chain Risks in a Procurement
Morgan Lewis

Understanding What You Want to Review

Every company or asset in a deal has supply chain cybersecurity risk, but not all such risks require the same level of diligence/review.

Always Consider a Baseline Level of Supply Chain Cyber Assurance in Any Procurement

High Dollar Risks (or High Profile/Disruptive Risks)

- Information breaches
  - Significant privacy breaches
  - Loss of proprietary information
  - Information subject to governmental information restrictions
- Legal requirements for cybersecurity, where applicable, such as:
  - Critical infrastructure owners/operators
  - Financial institutions
  - Health care providers
- Integrity of key company cyber assets
- Systems that threaten significant third-party harm (worst case scenarios)

Unique Characteristics of the Procurement

- All businesses have risks that form a rough baseline. What makes this business different that may create higher-than-normal risk in certain areas? Possible considerations:
  - Type of equipment (Off-the-shelf equipment vs. bespoke equipment)
  - Type of threat (Financial crimes, general disruption and mischief, state-sponsored)
  - Critical assets (Are there one or two key systems? Or does the company rely on a broad array of typical computer systems that provide significant resiliency?)
  - Location of vendors and sources of vendor-supplied goods and services (Is this a country with a history of supply chain exploitation?)
  - Official notices/warnings issued or provided by government agencies (does the company rely on vendors for which warnings have been issued?)
  - Does the company purchase solely from OEMs or authorized distributors and resellers?
  - Does the company have a supply chain cybersecurity policy and evidence it has been implemented?
  - Cost of replacement equipment if a supply chain security issue arises

Reasonably Discoverable

- Given the diffusion of the supply chain, it is often impossible, if not impractical, to examine all supply chain cybersecurity risks fully. In those circumstances, a diligence exercise needs to determine what level of risk is acceptable given the inefficiencies of identifying all risks. Considerations include:
  - Transparency of supply chain
    - Ability to provide a "bill of materials" or equivalent
    - Steps in supply chain and nature of buyer's relationship with suppliers
  - Ability of vendor to support good supply chain authenticity practices (e.g., software verification/authenticity)
  - Practicality of hardware examination
  - Leveraging internal or external audits/reviews to identify vulnerabilities
  - Cross-checking with National Vulnerability Database and similar resources
    - Is it off-the-shelf enough to be well-covered in public databases?
  - What can be quickly identified and fixed following a transaction

Mechanisms for Addressing Supply Chain Risk in Procurements

Pre-Transaction Reviews

- Review of certification documentation
- Cyber hygiene of vendor
- Identification of key suppliers and their cybersecurity risks
- Traditional diligence questions (such as a cybersecurity survey)

Deal Documents and Seller Commitments

- Representations
- Warranties
- Level of security protections provided (e.g. encryption of data in transit and storage)
- Existence and cost of patching support (functional vs. security)

Ongoing Reviews and Improvements

- Internal or third-party reviews
- Change in law issues, particularly in likely-to-be-regulated areas

Procurement Negotiations: Getting to "Yes" with Your Vendor or as a Vendor

Morgan Lewis

Company Concerns & Vendor Solutions

Vendor Noncompliance Will Be Expensive

- Can the vendor be compliant?
- Will the vendor cooperate in the security programs and take them seriously?
- Will the vendor share the cost of noncompliance with regulatory obligations?

Vendor Noncompliance Will Harm Others

- Does the vendor have strong security practices?
- Can the vendor cover the cost of damage it causes?
- Do our stakeholders trust this vendor?

Vendor Concerns & Company Solutions

Company Demands Will Drive Up Costs	• Can the company's current compliance program cover vendor personnel? (such as remote access) • What can be outsourced to the company?
We Cannot Comply with These Requirements	• Is this a learning curve issue? • Does the vendor have other clients with similar concerns?
The Risk Is Too Great	• How much risk does the company need its vendor to bear? • How likely is it that the vendor's scope of work could create significant liability for third-party harms? • Is there a statutory or regulatory bar on liability that could protect the vendor?

Getting to Yes on Risk Allocation

Risk Costs

- Regulatory penalties
- Enforcement costs
- Mitigation costs
- Damages (to equipment, to business, or from lawsuits)

Allocating Risk

- Price of service
- Indemnification (including replacement)
- Insurance
- Liability caps

Getting to Yes on Contract Language

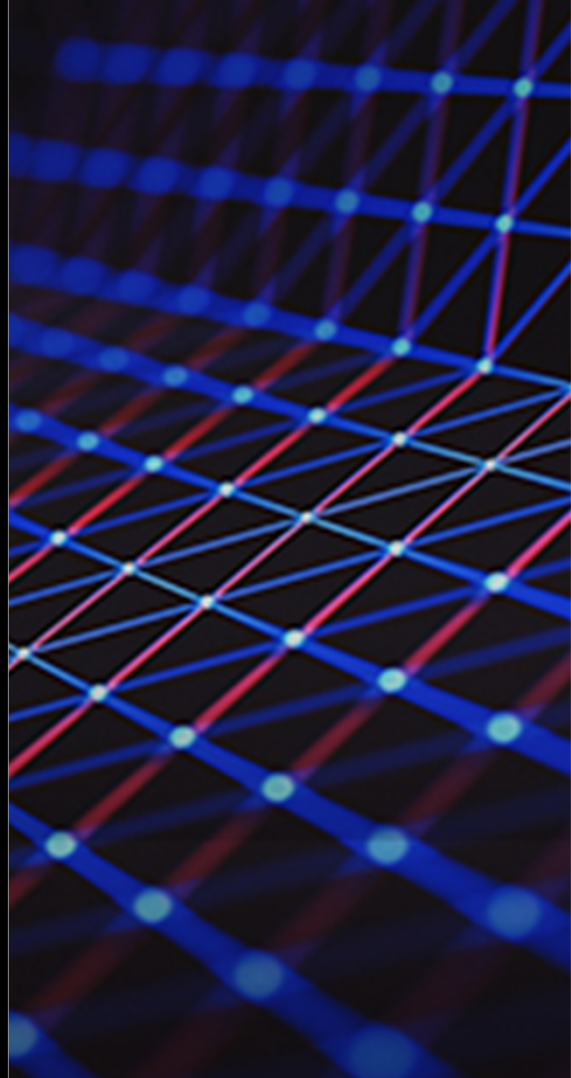
- Allocation of risk
- Security commitments and the costs of security activities
  - Specific contract language agreeing to security practices
  - Incorporating company policies where appropriate (physical access, remote access)
- Coordination in legal proceedings
- Coordination in incident response
- Indemnification process
  - Addressing replacement vendors
  - Cost of information breaches
- Confidentiality, publicity, and government information sharing
- Changes in law

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.



Morgan Lewis

Biography

J. Daniel Skees
Washington, D.C.
+1.202.739.5834
daniel.skees@
morganlewis.com

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, utility financing, electric markets and trading issues, reliability standards development and compliance, including cybersecurity requirements, administrative litigation, and transmission development. In handling appeals of FERC decisions, Dan has successfully represented clients before both the US Court of Appeals for the District of Columbia Circuit and the US Court of Appeals for the Fifth Circuit.

Biography

Robert Goldfin
Washington, D.C.
+1.202.739.5377
robert.goldfin@
morganlewis.com

Robert Goldfin represents major energy industry participants in regulatory and transactional matters, including enforcement proceedings and investigations. He handles Federal Power Act matters before the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). Robert advocates for clients before the Nuclear Regulatory Commission (NRC) and US Court of Federal Claims, and in settlements with the US Department of Energy (DOE) regarding spent nuclear fuel. He also represents clients on national security and international trade matters, including assisting US and foreign entities with notices to the Committee on Foreign Investment in the United States (CFIUS).

Biography

Arjun Prasad Ramadevanahalli
Washington, D.C.
+1.202.739.5913
arjun.ramadevanahalli@morganlewis.com

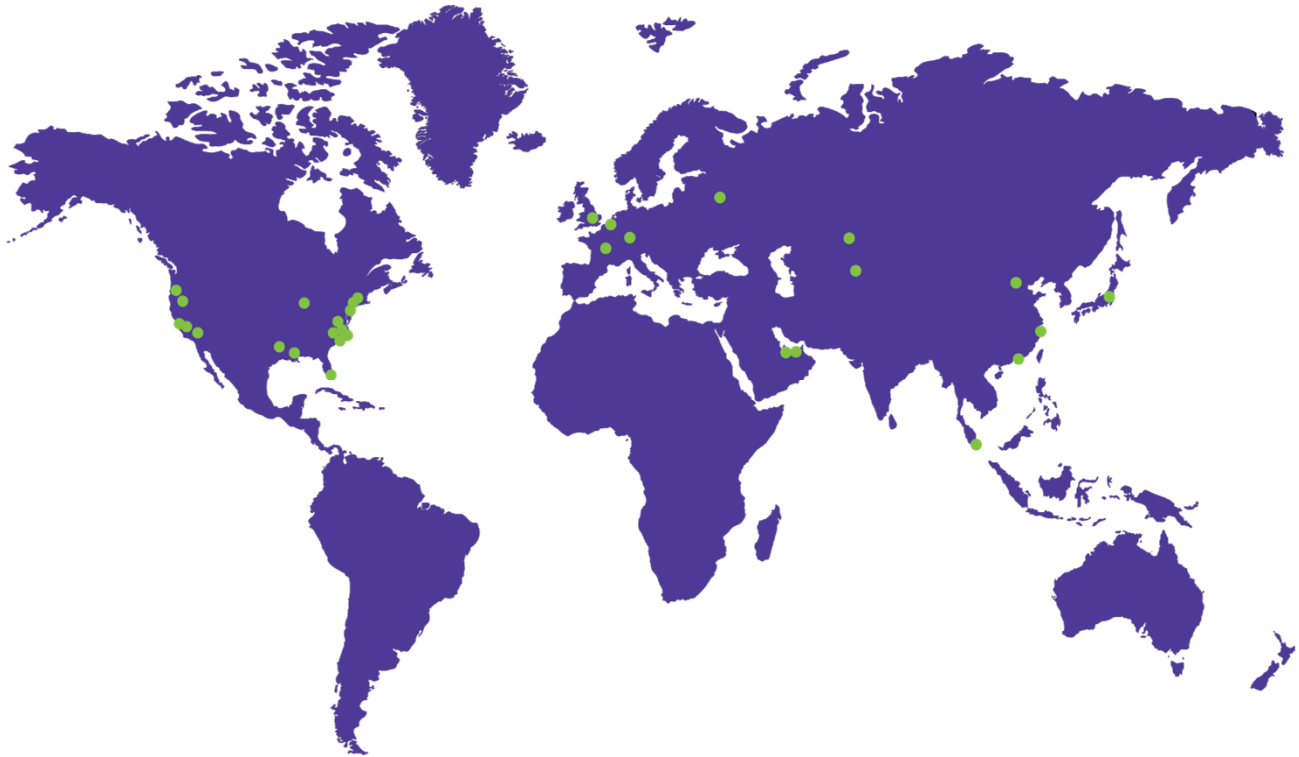
Arjun Prasad Ramadevanahalli represents electric power, natural gas, and oil industry participants in regulatory and transactional matters. He assists clients on issues relating to wholesale markets, utility transactions, rate matters, and enforcement proceedings before the Federal Energy Regulatory Commission (FERC). Arjun's practice also covers reliability standards enforcement and compliance matters before FERC and the North American Electric Reliability Corporation (NERC), including advising utilities on cybersecurity compliance and cybersecurity controls under the Critical Infrastructure Protection (CIP) suite of standards.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU