
Morgan Lewis
TECHNOLOGY MARATHON
National Cybersecurity Strategy: What Critical Infrastructure Owners Need to Know
Steve Spina, Robert Jacques, and Arjun Ramadevanahalli
May 25, 2023 | 1:00–2:00 pm ET
© 2023 Morgan, Lewis & Bockius LLP

Presenters

Steve Spina

Robert Jacques

Arjun Ramadevanahalli

Morgan Lewis

Agenda

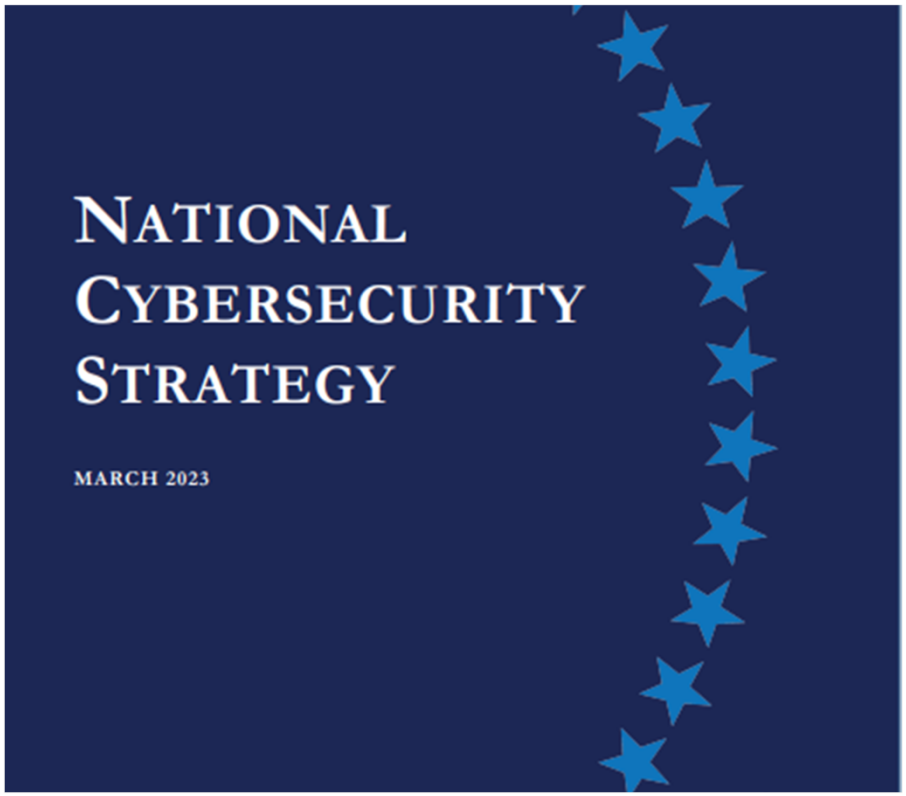
- National Cybersecurity Strategy Overview
- Implications for Critical Infrastructure Industries
- Cyberinsurance Backstop and Related Considerations
- What Happens Next?

National Cybersecurity Strategy Overview

Morgan Lewis

Overview

- White House strategy to reinvigorate federal government approach to cybersecurity
- Ambitious and wide-reaching strategic objectives centered around five "pillars"
- Calls for a rebalancing of cybersecurity responsibility and a realignment of long-term incentives



Trends Observed

- Deepening digital dependencies accelerated by emerging technologies
  - New possibilities, but also new risks
- Complexity in software and systems
  - Layering of functionality on "brittle systems" at the expense of security
- Increase in nation-state malicious activity
- Rapid changes to Operational Technology (OT) environments
  - Information Technology (IT)/OT convergence
  - Digitization of previously analog devices

Five Pillars

- **Pillar 1: Defend Critical Infrastructure**
- **Pillar 2: Disrupt and Dismantle Threat Actors**
- **Pillar 3: Shape Market Forces to Drive Security and Resilience**
- **Pillar 4: Invest in a Resilient Future**
- **Pillar 5: Forge International Partnerships to Pursue Shared Goals**

Implications for Critical Infrastructure Industries

Morgan Lewis

Critical Infrastructure Takes Center Stage

- Strategic Objective 1.1: Establish Mandatory Cybersecurity Requirements
  - Recognition that "the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes"
- Major policy change for the federal government
  - Prior efforts have been intensely focused on voluntary measures, public-private collaboration, and a "light touch" with industry
- Recommendation for performance-based regulations that leverage existing cybersecurity frameworks, voluntary standards, and guidance
- Significant challenges for federal agencies
  - Jurisdictional limits
  - Workforce
  - Overlapping requirements

Pros and Cons of Mandatory Regulation

Accountability	Limits entity discretion
Litmus test	"One size fits all"
Access to insights	Costs
Socialization of best practices	Administrative burden
Cost recovery	Disclosure risks

Case Study:
Transportation Security Administration Cybersecurity Rules

Key Implementation Challenges	
Scoping (What's in? IT vs. OT?)	Timing
Overlapping regulations (e.g., NERC CIP)	Lack of clarity on rights and process
Mitigation strategies	Cost-benefit
Vendor/supply chain issues	Cost Recovery (Regulated Utilities)

Other Relevant Strategic Objectives

- A congressionally directed engineering strategy for clean energy technology, such as distributed energy resources
- Adoption and enforcement of a risk-based approach to cybersecurity across infrastructure-as-a-service (IAAS) sectors to prevent malicious actors from exploiting US-based infrastructure (e.g., cloud infrastructure)
- An enhanced focus on the pernicious threat of ransomware attacks, which have targeted critical infrastructure and essential services
- Development of national data privacy legislation to drive greater accountability for organizations holding and using sensitive data, such as personal, health, and geolocation information
- Development of legislation establishing liability for software products and services
- Incentivizing the adoption of secure software development practices, including the development of software bills of material (SBOMs) to support supply chain risk mitigation
- Assessing the need for a federal cyber insurance "backstop" mechanism in response to catastrophic cyber events
- Using international coalitions to reinforce global norms of "responsible state behavior," such as refraining from cyber operations that would intentionally damage critical infrastructure

Cyberinsurance Backstop

Morgan Lewis

Strategic Objective 3.6: Cyber Insurance Backstop

- Cyber Security: risk management process (rather than an end-state) to continuously:
  - identify and protect against potential cyber security incidents
  - detect, respond to, and recover from actual cybersecurity incidents
- Cyber Insurance: component of "Cyber Security" + broad term for insurance policies that cover liability or direct losses from events adversely affecting electronic activities / systems
  - Part of traditional insurance coverage vs.
  - Standalone policies with various coverages

1st Party (Direct Losses)	3rd Party (Liability Losses)
❑ Electronic data protection ❑ Cyber event management ❑ Business interruption ❑ Cyber extortion ❑ Cyber crime	❑ Network security liability ❑ Privacy liability ❑ Electronic media liability ❑ Technology E&O liability ❑ IP liability

Strategic Objective 3.6: Cyber Insurance Backstop

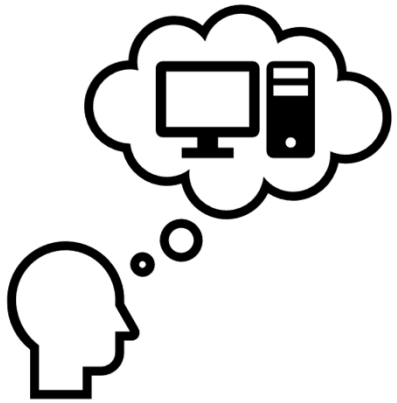
- Objective to "shape market forces to drive security and resilience"
- Potential iteration of partnership b/w gov't and insurance industry for certain risks:

	Nat'l Flood Ins. Program (1968)	Terrorism Risk Ins. Act (2002)
Program Description	FEMA sets rates and largely funds, while insurers issue policies and service claims	Cost-sharing mechanism (post-9/11) for certified terrorism events resulting in losses of $200M+
Nature of Loss	Relatively understood risk subject to actuarial assessment	Infrequent, highly unpredictable losses
Market Problem Addressed	Prohibitive cost for policyholders, leading to un/under-insured property owners	Insurer reluctance to issue coverage (USA 80% responsible for covered losses)
Notable Loss Control Reqs.	Floodplain management plans	None

Strategic Objective 3.6: Cyber Insurance Backstop

- The state of affairs for cyber:

	Cyber Insurance Backstop (Under Consideration)
Nature of Loss	Cyber risk is constant (relatively frequent), but novel, difficult to assess actuarially, and constantly evolving
Problems to Address	1. Relatively limited actuarial understanding / pricing reliability 2. Relatively high frequency and potentially high loss (systemic) events 3. Variety of actors, motivations, and types of cyber threats 4. Enough companies with deficient cyber hygiene / processes 5. National security / economic implications 6. Lack of standardization / consistency among insurance policies 7. Potentially material coverage gaps or minimal limits 8. Not an obvious value / priority for some businesses: a) Prohibitively costly b) Unproven product (with high-profile coverage litigation) c) "Won't happen to me"
Loss Control Reqs.	To be decided… but any government-supported private framework should incentivize companies to meet meaningful cyber hygiene standards ("safe IT administrator discount")



Structure and scope of federal program in exploratory (preliminary) stage

Strategic Objective 3.6: Cyber Insurance Backstop

- Benefits to **Insurers**:
  - Financial certainty and stability
  - Potential mechanism for more standardization and data sharing
- Benefits to **Insured Companies**:
  - More affordable and more available coverage (increased supply)
  - Potential for more standardized and/or better terms (better quality)
- Benefits to **Government/Public**:
  - Increased prevalence of cyber insurance (market stability)
  - More sophisticated, resilient society (underwriting and loss control)
  - Potential for improved data sharing among private / public actors

What Happens Next?

Recent Federal Initiatives

- DHS CISA guidance
  - Software bill of materials (SBOM)
  - Updated cross-sector Cybersecurity Performance Goals (CPGs)
- Securities and Exchange Commission – Proposed Requirements
- Environmental Protection Agency – Memorandum for Public Water Systems
- Expansion of Transportation Security Administration Security Directives
- And others . . . .

What Can Critical Infrastructure Owners Do Today?

Policy Advocacy

- Participate in stakeholder opportunities to shape requirements (before formal rulemaking where possible)
- Regulator education is key

Interdisciplinary

- Achieving compliance requires coordination among IT/OT; security, compliance, and legal
- Shortchanging one or the other creates risks

Cultural Change

- Ensure that cybersecurity is taken seriously throughout the organization and at the highest levels

Existing Tools

- Use non-binding guidance and best practices to shore up cyber posture

Mandatory requirements = steep learning curve, timing challenges, legal risk

Leveraging Non-Binding Guidance to Fill Gaps

- Mandatory and enforceable requirements do not always cover each issue, or may not at first
- NIST guidance, even if aimed at federal agencies, can:
  - Fill in the gaps between mandatory requirements and comprehensive protection
    - Provide content
    - Check for gap identification
  - Provide a preview of what may become enforceable
  - Serve as a useful guide when contracting
  - Standardization on highly technical areas
- Key examples include:
  - NIST Cybersecurity Framework
  - NIST SP 800-161 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations)
  - NIST Federal Software Procurement Guidance

Challenges

- Greater legal accountability requires legislative action
  - Political divisions compound the challenge
- Agencies in jurisdictional "grey areas"
- Light on implementation details
  - Further updates are forthcoming from the White House
- Harmonizing duplicative or overlapping requirements
  - Strategy recognizes the negative impacts of duplicative or conflicting regulatory requirements
  - Directs regulators to "work together to minimize these harms," but it is unclear how such harmonization will occur in practice

Biography

Stephen M. Spina
Washington, D.C.
+1.202.739.5958
stephen.spina@morganlewis.com

Stephen M. Spina is a leader of the energy and project development practice. Steve represents electric utilities and other electric industry participants before the Federal Energy Regulatory Commission (FERC) in restructuring, market investigations, and Federal Power Act regulatory matters. He advises electric utilities on issues relating to market pricing, transmission, reliability standards compliance (including cybersecurity standards), rate matters, and participation in regional transmission organizations, including capacity and energy market issues. In connection with cybersecurity and electric reliability, Steve is an active member in the firm's crisis management practice. His work also extends to audits and investigations before FERC's Office of Enforcement, as well as enforcement and audit proceedings involving the North American Electric Reliability Corporation.

Biography

Robert Jacques
Washington, D.C.
+1.202.739.5217
robert.jacques@morganlewis.com

Robert Jacques is a commercial litigator with deep insurance knowledge. He has handled more than $1 billion in claims under various types of policies, including cyber, directors' and officers' liability (D&O), commercial general liability (CGL), environmental, product recall, errors and omissions (E&O), and property/business interruption. Apart from litigating large claims with virtually every major carrier, Robert writes, comments, and presents on complex coverage issues, informed by his certifications as a chartered property casualty underwriter (CPCU) and associate in claims (AIC).

Biography

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

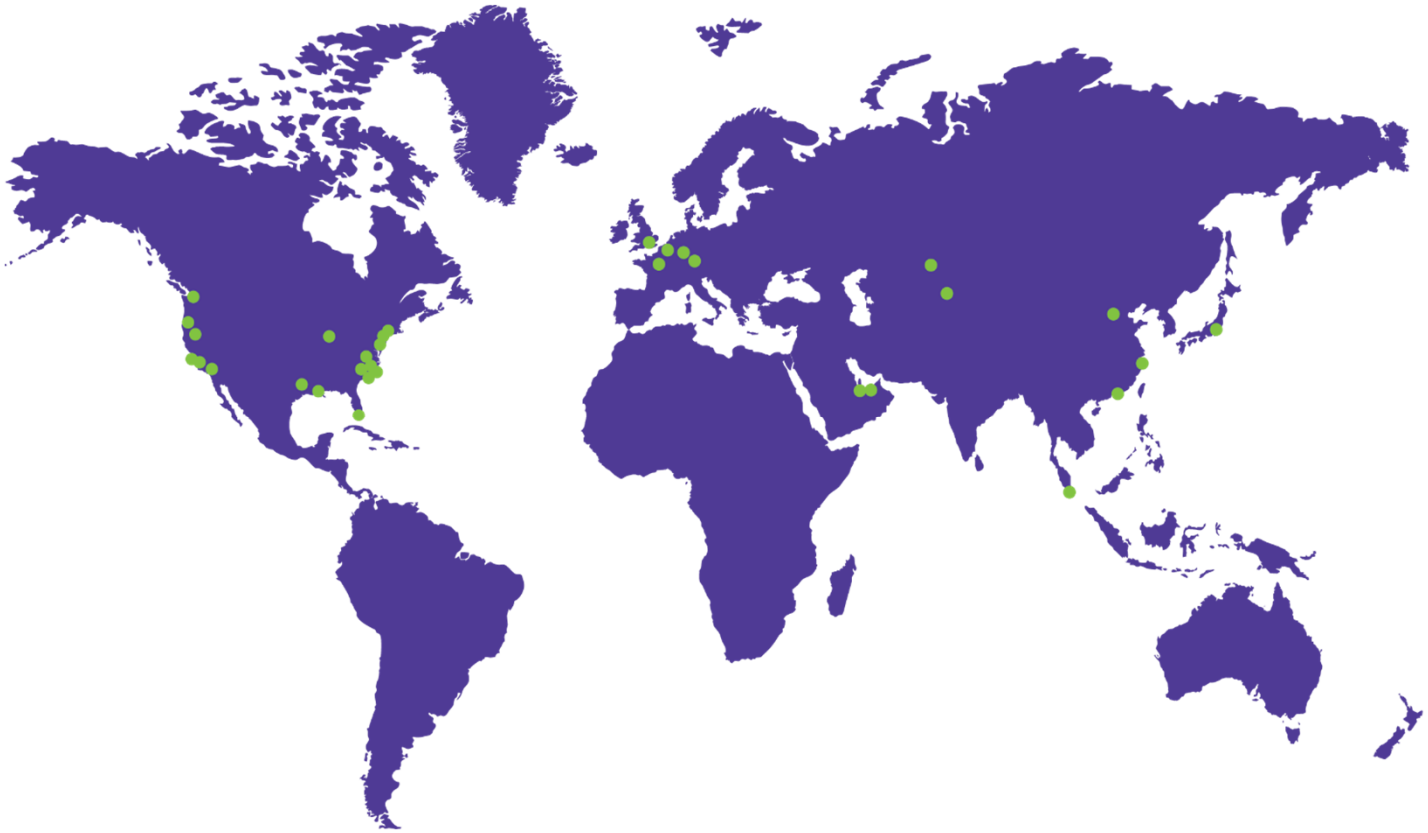
Arjun Prasad Ramadevanahalli represents electric power, natural gas, and oil industry participants in regulatory and transactional matters. He assists clients on issues regarding wholesale markets, utility transactions, rate matters, and enforcement proceedings before the Federal Energy Regulatory Commission (FERC), and on cybersecurity matters in the energy industry. Arjun regularly advises utilities and other industry participants on North American Electric Reliability Corporation (NERC) reliability standards enforcement and compliance matters, including cybersecurity compliance and controls under the Critical Infrastructure Protection (CIP) suite of standards. Arjun counsels pipeline owners and operators on cybersecurity compliance before the Transportation Security Administration (TSA).

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

THANK YOU