The U.S. Cybersecurity Regulations Mismatch – Why Deregulation Cannot Solve Cybersecurity Regulations Disharmony

Problem Statement and Goals

Problem Statement:
Despite consensus on the need for regulatory harmony, U.S. cybersecurity regulations remain deeply fragmented, with conflicting requirements and directions at the state, federal, and international levels.

As federal deregulation accelerates in 2025, this research asks: Will deregulation solve the harmonization problem or make it worse?

Goals:

- Identify the root causes (drivers) of regulatory disharmony in U.S. cybersecurity regulations
- Analyze how federal deregulation and post-Loper Bright legal uncertainty affect harmonization efforts
- Offer actionable recommendations for improving regulatory coherence and a pathway for cybersecurity regulatory harmonization

Approach

Two-Phased Research Design

Phase 1 (2024)
Identifying Drivers of Disharmony

Research Question: Why does government keep producing disharmony despite consensus on need for harmony?

Key Activities:
- Systematic regulatory document analysis
- Classification of 8 drivers (5 internal, 3 external)

Phase 2 (2025)
Deregulation Impact Analysis

Research Question: Will deregulation solve the harmonization problem or make it worse?

Key Activities:
- Policy shift tracking (Biden → Trump admin)
- Post-Loper Bright legal uncertainty analysis

Research Methodology

Data Sources Analyzed

- Federal regulations (CIRCIA, SEC, FTC, TSA, FCC)
- Industry stakeholder comments (ONCD RFI)
- State & international frameworks (NY, CA, EU)
- Legal precedent (Loper Bright)

Analytical Framework

- Driver classification (internal vs. external)
- Policy comparison (Biden vs. Trump approaches)
- Legal vulnerability assessment
- Regulatory mismatch analysis

Results

Not All Cyber Regulatory Disharmony Is Equal

Eight drivers account for persistent cybersecurity regulatory disharmony. Internal drivers reflect bureaucratic structures and decision-making, often increasing compliance costs, while external drivers respond to sectoral, technological, and geopolitical risks and can, in some cases, improve security outcomes

Drivers of Disharmony in Cyber Regulations	
Internal to Each Regulator	**External**
Unique authorities and public-policy purposes	Lack of centralized governance and frameworks
Precedents to other regulations or bureaucratic processes	Sector and Company-Specific Tailoring of Regulations
Desire for sovereignty or organizational autonomy	Evolving risk profiles due to geopolitical events and rapid tech shifts
Uneven distribution of expertise and information	
Bureaucratic inertia and particularities	

Deregulation Deepens Disharmony Rather Than Resolving It

Recent deregulatory shifts have altered the structure and stability of U.S. cybersecurity regulation. These findings show how domestic legal uncertainty cascades into international divergence and intensifies the need for regulatory harmonization.

Finding 1: Deregulation Does Not Reduce Cyber Regulatory Complexity

- Federal retreat does not reduce complexity
- State proliferation fills the vacuum
- Coordination capacity declines

Finding 2: Heightened Legal Uncertainty After *Loper Bright*

- Agency authority now unpredictable
- Regulations with indirect statutory basis vulnerable
- Courts become arbiters across jurisdictions

Finding 3: International-Domestic Mismatch Widens

U.S. (Fragmenting)	EU (Harmonizing)
Federal retreat + State proliferation	NIS2, DORA, Cyber Resilience Act

Multinationals must comply with highest global standard

Finding 4: Deregulation Will Make Harmonization Increasingly Necessary

- Industry consensus emerging on need for harmonization, but voluntary alignment insufficient
- Coordination mechanisms and clear legal authority required for effective harmonization

KEY RECOMMENDATIONS

- **Appoint Assistant National Cyber Director for Regulatory Strategy**
- **Create a Harmonization Committee and Regulatory Clearinghouse**
- **Create ONCD Office for Regulatory Matters**
- **Develop Mutual Recognition and Frameworks with International Partners**

Samuel Dab
School of International & Public Affairs, Columbia University
COLUMBIA | SIPA School of International and Public Affairs

The U.S. Cybersecurity Regulations Mismatch – Why Deregulation Cannot Solve Cybersecurity Regulations Disharmony

Abstract

U.S. cybersecurity regulation suffers from severe fragmentation at federal, state, and international levels, with overlapping requirements forcing organizations to dedicate excessive resources to compliance navigation rather than defense. This research conducts a two-phase analysis: first identifying eight "drivers of disharmony" (five internal, three external) that systematically produce regulatory inconsistency, then examining how federal deregulation affects these drivers.

Internal drivers like bureaucratic inertia create arbitrary differences that harm security outcomes, while external drivers like sector-specific tailoring can be beneficial but require coordination. The regulatory landscape grew dramatically more complex in 2024-2025 as the Supreme Court's Loper Bright decision eliminated Chevron deference and the Trump administration pursued aggressive deregulation, reducing CISA's workforce and substantially reducing its purview. Simultaneously, U.S. states accelerated rulemaking while the EU advanced harmonization through NIS2, DORA, and the Cyber Resilience Act.

This creates a "regulatory mismatch": federal retreat, state proliferation, and international coordination moving in opposite directions. While strategic deregulation and consolidation can support harmonization when coordinated, our findings show that deregulation without harmonization mechanisms deepens fragmentation rather than resolves it.

We recommend appointing an Assistant National Cyber Director for Regulatory Strategy to lead a Harmonization Committee, establishing regulatory clearinghouses, and pursuing bipartisan legislation. Effective cyber defense requires not less regulation, but smarter, harmonized regulation backed by legislative clarity.

This research project also led to the development of a newsletter on cybersecurity regulations, written, edited and published by students from the SIPA Cyber Program at Columbia University.

COLUMBIA | SIPA
Cyber Regulations Watch

Grateful acknowledgment to Jason Healey, Columbia SIPA and SIPA Cyber, for his mentorship and guidance.

Samuel Dab
School of International & Public Affairs, Columbia University

COLUMBIA | SIPA
School of International and Public Affairs