Prepared Statement

Jason Healey

Columbia University's School of International and Public Affairs

For the United States House Committee on Oversight and Accountability

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

25 July 2024

Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to share my observations on Enhancing Cybersecurity by Eliminating Inconsistent Regulations, as well as for your leadership on cybersecurity issues. My name is Jason Healey, and I am a senior research scholar at Columbia's School of International and Public Affairs.

The White House, Congress, and business all agree that the harmonization of cyber regulations – by eliminating those which are inconsistent, improving reciprocity between regulatory agencies, or other means – is one of the most important topics in cybersecurity.

Everyone agrees for regulatory harmonization, and no one calls for disharmony. But here we are, stuck with inconsistent, unharmonized regulations. Even if legislators and regulators trim back all the inconsistent regulations today, they will grow back unless we identify the sources of disharmony that keep delivering unharmonized regulations. So how do we end up with disharmony?

Our research at SIPA's Cyber Regulation Lab, has been investigating the harmony and disharmony of cyber regulations. And while our work is still in relatively early stages, we have initial insights to share, especially on nine "drivers of disharmony." Four of these are internal to each regulator, as shown in Table 1, while five are external.

Table 1: Drivers of Disharmony in Cyber Regulations	
Internal to Each Regulator	**External**
Unique authorities and public-policy purposes	Tailoring for sectors and companies
Precedents to other regulations or bureaucratic processes	Companies operating in different sectors
Desire for sovereignty or organizational autonomy	Geopolitical events change risk profiles of sectors differently
Bureaucratic inertia and particularities	Rapid tech shifts change risk profiles of sectors differently
	Lack of centralized governance and frameworks

Internal Drivers

Though the four internal drivers of disharmony arise from the everyday bureaucratic idiosyncrasies, they are often far less defensible than the external drivers.

The best example of **unique authorities and public-policy purposes** driving disharmony must be incident reporting timelines. When Colonial Pipelines was affected by ransomware, the Department

of Homeland Security (including the Transportation Security Administration and Cybersecurity and Infrastructure Security Agency) needed to know very quickly, so they could assess the potential impact on public health and safety and to enhance situational awareness across critical infrastructure sectors.

The timelines are far more relaxed for understanding cumulative impact over time, such as assessing the effectiveness of security controls or informing the insurance and reinsurance industries. Rather than hours or days, that information can usually trickle in over weeks and months with little impact.

Both sets of goals were included in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and both have the short mandates of reporting within 72 hours after a reasonable belief that a "covered cyber incident has occurred." CISA asked for even shorter deadlines, just 24 hours, for submission of a Ransom Payment Report.

Inconsistencies also arise from when regulators rely on **different internal precedents and processes**. For example, in 2023 the Securities and Exchange Commission perhaps had little choice but to mandate a four-day reporting timeline for public companies, once an incident was determined to be material by the company's board. Four days is the timeline for reporting of any kind material incident, so SEC stood by that precedent, even though the New York Department of Financial Services' mandate for 72-hour reporting dates to 2017 and the Federal banking regulator's 36-hour requirement dates to 2021.

Internationally, the Waasenaar Arrangement, fulfilling their arms-control mandate, almost "inadvertently outlawed much of the business that's done across the global cybersecurity industry."

An uglier example of internal precedents and processes is the SEC's attempted prosecution of the Chief Information Security Officer of SolarWinds. Even though the rest of the government was encouraging companies to treat cybersecurity as a matter for the board and CEO, the SEC decided to only go after the CISO, who is almost universally the overworked internal champion of security.

To examine **sovereignty and organizational autonomy**, let us look at state data-breach notification laws, which widely differ not just on the when of reporting, but the how. When customers' sensitive personal information has been stolen, different states have mandated customers should be notified anywhere from "without unreasonable delay" to no later than 60 days after discovery. New Jersey's breach notification law requires notification to State Police prior to notifying consumers, while Virginia mandates simultaneous notification to the state Attorney General and consumers. More broadly, in their response to the Request for Information from the Office of the National Cyber Director, the Insurance Coalition quoted from the National Conference of States Legislature that "at least 25 states enacted 43 new cybersecurity laws in 2022, out of 250 bills proposed by at least 40 state legislatures."

Lastly: **bureaucratic inertia and particularities.** As Jim Dempsey has explained in Lawfare, regulators developed different security controls for ostensibly similar purposes. These changes seem to be entirely because of idiosyncratic choices made by each regulator rather than carefully being tailored for each sector (see next section).

For example, CISA's Cybersecurity Performance Goals "have a section on supply chain risk, a topic not covered at all" in TSA's directive on pipeline security. The reverse is true as well, as the TSA

directive "has controls not mentioned in the CPGs, such as the capability to monitor or block connections from known or suspected malicious command-and-control servers."

External Drivers

Other drivers of disharmony are external to the regulator.

Most obviously, **differences between sectors and companies** should result in different, tailored regulations. Facing similar threats, banks are heavily regulated, and casinos are not. Any particular regulation, such as mandatory reporting of an incident within 72 hours, may be far too quick for some sectors but too delayed for others. Even sectors with a similar threat profile, and which impose the same impact on the United States if disrupted, could have different, tailored regulations if they had different capacities to deal with those regulations. Some sectors just are more used to dealing with regulations (compare say, bulk electricity versus water and wastewater) or have more resources to deal with them.

These effects also can apply to particular companies. Some, such as Systemically Important Financial Market Utilities or Global Systemically Important Banks, are deemed by regulators to be so critical to a particular sector they require additional rules. The "Section 9" entities (so named from that section of Executive Order 13636) are those, in whatever sector, against which "a cybersecurity incident could reasonably result in catastrophic regional or national effects." The same concept underpins CISA's work on Systemically Important Entities, work which I helped spearhead. When sectors, and some companies within sectors, are treated differently, there will also be opportunities for disharmony and inconsistency.

The resulting disharmonies are far worse for **companies operating across different sectors with different rules**. Companies in aviation and the Defense Industrial Base are especially affected by this. As a sector, the DIB is the only one defined solely by its customer, the Department of Defense, and not their products or services they provide.

As the National Defense Information Sharing & Analysis Center wrote in response to the ONCD RFI, "as companies that span multiple U.S. critical infrastructure sectors and International environments … defense contractors are often subjected to multiple incongruent cyber requirements across a multitude of varying cyber frameworks." Likewise, the aviation industry noted they could be subject to 11 different incident reporting frameworks of federal departments and agencies.

Geopolitical and technological changes can also create disharmonies, especially when rapid.

After the full-scale Russian invasion of Ukraine, CISA worked with the DoD to identify the entities which might be most likely to come under attack. Though this, to my knowledge, did not lead to any additional regulatory requirements, it is reasonable to imagine additional burdens on those companies in the U.S. critical infrastructure which would be most likely to be attacked, should China decide to invade Taiwan.

As for technological changes, Artificial Intelligence seems likely to stress the regulatory system, disproportionately impacting different sectors at different paces. But the effect is fairly widespread. In their response to the ONCD RFI, the World Economic Forum noted that since "federal regulations

in the US electricity sector focus on bulk distribution," those rules will need to change as renewable energy becomes ever more important to the U.S. economy.

Lastly, there is a **lack of centralized governance mechanisms** and frameworks – both within the United States and globally. The proposed Cybersecurity Regulation Harmonization Act would establish a Harmonization Committee, which would help, as has existing work by the Cybersecurity Forum for Independent and Executive Branch Regulators. But there may be far too many regulations, governed by far too many agencies (and congressional committees) for such a committee to succeed unless substantially empowered.

Frameworks are another key step to better governance and harmonization. Many of the existing frameworks are at the level of individual cybersecurity controls (which as Jim Dempsey points out can have anywhere from 36 to nearly 1,200 separate controls). Other frameworks are needed, such as to assess whether regulations are performance based (that is, are both rules based and seek specific outcomes, such as mandating "recovery within two hours after an event") or management based (general and only mandating specific behaviors, such as "recovering in a timely manner").

As I explained in a 2023 article in Lawfare, performance-based regulations are among the hardest to harmonize – because differing regulators have to agree on the specifics – and are only useful when the results can be measured. Management-based and the related principles-based regulations "give regulated entities flexibility in how best to achieve a desired objective," according to Heath Tarbert, then-head of the U.S. Commodity Futures Trading Commission.

Frameworks can also provide clarity to the regulatory process, by helping regulators specify *exactly which market failures their regulations are meant to fix*. Mandatory reporting requirements are fixes for the market failure of information asymmetries. Investors lack the understanding of corporate insiders, so the SEC requires reporting of material incidents. The government and downstream customers lack information about the cascading impact of ransomware events like Colonial Pipeline, so CIRCIA will mandate reports within 72 hours.

By comparison, baseline cybersecurity requirements are fixes for the market failure of negative externalities. Because there was such a cascading impact from the disruption at Colonial Pipelines, regulators felt it necessary to impose a minimum baseline of security. Same incident, different market failure, different kind of regulation. Our Cyber Regulation Lab will be publishing more on market failures over the coming months.

Analysis and Recommendations

Congress and the executive branch – including independent regulatory agencies – must eliminate inconsistent regulations but also go after the source of the problem, tackling these drivers of disharmony. Else new, inconsistent rules will continue to proliferate, even as old ones are removed. To do so, we at the Cyber Regulation Lab have several recommendations.

First, we encourage passage of a strong Cybersecurity Regulation Harmonization Act, including provisions for authorities, staffing, and funds for the interagency Harmonization Committee. The Act should also be broadened to not just minimum baselines (a fix for the market failure of negative externalities) but a wider range of actions. These might include liability and ex-post investigations, such as the misguided (and ultimately rejected) charges against the SolarWinds CISO.

Second, congressional committees can review where legislation might be overly specific (such as mandating reporting within 72 hours, per CIRCIA) or not specific enough. This is especially important with the Supreme Court's decision in *Loper Bright*.

Third, regardless of the status of the Cybersecurity Regulation Harmonization Act, ONCD should not only create a new office for regulatory matters, run by a dedicated assistant national cyber director, but also publish a regulatory strategy. Regulation is more inherently political than most other cybersecurity initiatives, such building the cyber workforce. Which has a dedicated strategy (subordinate to the National Cybersecurity Strategy) and a dedicated office. ONCD should, in the early days of the next administration, lay out major options for ultimate approval of the principals of the National Security Council and National Economic Council.

Fourth, and again regardless of the status of the Act, ONCD should lead executive branch efforts on cyber regulatory frameworks. These frameworks should not just cover specific controls but the categories of regulations and specific market failures. As a reminder from the above section: regulatory harmony is far easier with management- and principles-based regulations.

Lastly, we researchers need to do a better job of understanding which regulations are most effective, in which circumstances, and at the least cost. Until we do so, the federal government may default to rules which while harmonized, are ultimately ineffective. Our lab is beginning to provide honoraria for researchers to republish their academic papers on these topics for more policy-focused websites.

Conclusion

As I wrote last year, more than 50 years ago, an influential task force concluded that it was impossible to adequately secure computers and networks from cyberattacks unless they were entirely closed off from the outside world. Attackers, not defenders, generally have the advantage. Regulation will be an important step to fixing these problems, so our grandchildren do not face the same issues as we face today, and as our grandparents faced before us.

The White House's National Cybersecurity Strategy, which I was honored to help draft, calls for "modern and nimble regulatory frameworks for cybersecurity" that are both "tailored for each sector's risk profile [and] harmonized to reduce duplication." These two goals can pull in different directions and require constant attention, such as by this subcommittee.

These findings by our lab are still in the early phases. We thank our sponsors who have supported this work and appreciate the work of our student researchers, including Samual Dab, Tarang Jain, Carina Kaplan, and Christine McNeill. We look forward to continuing to work with the sub-committee members and its staff as we continue our important work on harmonization and the elimination of inconsistent regulations.