REGULATORY DIVERGENCE: FAILURE OF THE ADMINISTRATIVE STATE

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTERGOVERNMENTAL AFFAIRS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 18, 2018

Serial No. 115–92

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

31–369 PDF WASHINGTON : 2018

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana
Michael Cloud, Texas

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Jimmy Gomez, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Stacey E. Plaskett, Virgin Islands
John P. Sarbanes, Maryland

SHERIA CLARKE, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
KELSEY WALL, *Professional Staff Member*
KATY ROTHER, *Intergovernmental Affairs Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON INTERGOVERNMENTAL AFFAIRS

Gary Palmer, Alabama, *Chairman*

Glenn Grothman, Wisconsin, *Vice Chair*
John J. Duncan, Jr., Tennessee
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Walker, North Carolina
Mark Sanford, South Carolina

Jamie Raskin, Maryland, *Ranking Minority Member*
Mark DeSaulnier, California
Matt Cartwright, Pennsylvania
Wm. Lacy Clay, Missouri
(Vacancy)

CONTENTS

REGULATORY DIVERGENCE: FAILURE OF THE ADMINISTRATIVE STATE

Wednesday, July 18, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTERGOVERNMENTAL AFFAIRS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:08 p.m., in Room 2154, Rayburn House Office Building, Hon. Gary J. Palmer [chairman of the subcommittee] presiding.

Present: Representatives Palmer and Raskin.

Mr. PALMER. The Subcommittee on Intergovernmental Affairs will come to order. Without objection, the presiding member is authorized to declare a recess at any time.

The Federal Government has long been associated with entrenched bureaucracy, separated by agencies and ignorant of the realities of the average American's life. Federal agencies impose regulatory requirements under a siloed organizational structure that is program by program, department by department, with very little interagency coordination. This committee is well aware of the impact of Federal agencies' failure to coordinate between themselves and non-Federal stakeholders.

For the last 8 years, the Government Accountability Office has issued an annual report on overlapping, duplicative, and otherwise wasteful Federal programs. And to date, addressing the problems that GAO highlights in these reports has saved over $175 billion. Addressing the remaining could save tens of billions of dollars more. And I might even argue, in some cases hundreds of billions of dollars more.

In other words, the failure of Federal agencies to coordinate has wasted hundreds of billions of dollars of taxpayer money over the last decade.

But the impact of the failure of the administrative state doesn't stop there. The lack of interagency coordination has led to a steady accumulation of divergent regulatory mandates on States and the private sector. Despite often seeking similar results, Federal agencies impose conflicting regulations that force the regulated entities, like State agencies and private sector businesses, to focus heavily on compliance rather than improved outcomes.

Although the panel comes from different sectors, missions, and backgrounds, there is remarkable consistency in their testimony about the burdensome effects of a divergent regulatory regime.

Today Federal regulations touch nearly every aspect of daily life, and those regulations have become so complex that even the regu-

lators can't agree what the requirements are or how to comply with them.

As a result, these divergent regulations drastically increase the overall cost of the intended operations and deviate from the intended purpose of the regulations themselves. According to the Competitive Enterprise Institute, Federal regulations cost the economy nearly $2 trillion annually.

And what I like to point out, I have some colleagues who identify that as a hidden tax. It really isn't. At least a tax goes to build a road or a bridge or has some good purpose in many cases. A regulatory cost is just a hidden cost that weighs disproportionately heavily upon low-income families. I think that averages almost $15,000 per household.

Likewise, State governments also experience a drain on resources and State autonomy due to regulatory divergence. State officials from the National Association of State Chief Information Officers have shared multiple accounts with the committee on duplicative and inconsistent audit requirements imposing significant burdens on States without any substantive benefit.

One State's chief information security officer reported than an audit of the same data security enterprise yielded inconsistent results across multiple Federal agencies. Unfortunately, this has become a regular feature of the State partnership with the Federal Government.

It is our duty to the American people to explore opportunities to harmonize our current regulatory standards. To do this, Federal agencies, along with State governments and the private sector, need to come together to develop means of communication and cooperation to mitigate future duplicative, inconsistent, and obsolete regulations.

We are fortunate today to have with us a panel that can help us better understand the challenges imposed by these Federal regulatory standards. I thank the witnesses for being here today.

And at this point, I would like to yield to my friend and colleague from Maryland, the ranking member, Mr. Raskin, for his opening statement.

Mr. RASKIN. Mr. Chairman, thank you. It's always a pleasure to be with you, Chairman Palmer.

I'm planning to surprise everyone by becoming the first American politician in history to defend regulation in its entirety: the notice and comment period, the hearing process, regulatory enforcement, the whole kit and caboodle.

Let's start with terminology. A regulation is just a fancy name for a rule, and we all live according to rules. Every family has rules, every household, every sport, every school, every road, every highway, every institution, every economy, every government, every nation, every corporation, every State, county, city, and town.

And, indeed, Congress itself and every committee has rules. I get 5 minutes to do my opening presentation no matter how brilliant it is, not 6 minutes, not 4 minutes, but we've got a rule about it. The rule gives us a fair allotment of time and makes each of us free to use it. We will probably invoke dozens of rules as we go about our business in the House today.

But the rules targeted for criticism in this hearing are the rules that Federal agencies adopt to enforce the laws that we pass in Congress. The laws and the rules reflect the values of the people and implement our social priorities.

Look at what agency rules do. The Department of Labor's overtime rule says that hourly wage workers must be paid time and a half when their bosses ask them to work more than 40 hours a week. That's a rule which gives dignity and fairness to workers.

The Federal Aviation Administration's 24-hour rule says passengers forced to cancel airline ticket reservations with 24 hours of purchase must get a full refund. Another FAA rule says that passengers who miss their flight must be given standby access if they arrive within 2 hours of the missed flight on the next flight.

A lot of Federal rules save human lives and protect public health. The National Highway Transportation Safety Administration's Gulbransen rule requires dramatically improved rear visibility in new cars, which is why so many people in this room and in our country have backup cameras on their dashboards now. Although President Bush signed it into law in 2008, the rule was unnecessarily delayed and went into effect in 2018.

Named for 2-year-old Cameron Gulbransen, who was killed when a car accidentally backed up over him, this rule has already begun to significantly lower the number of deaths and injuries, roughly 250 deaths and more than 12,000 injuries a year that were occurring from accidents caused by vehicles in reverse. The rule compels use of a technology that had been available for a decade but was opposed by the auto industry, which tried to keep it as an optional luxury add-on item.

Everyone knows that the seatbelt rule has saved tens or even hundreds of thousands of lives since it was adopted in 1983 despite vehement protests that this was overregulation or hyper-regulation when it was first adopted.

Like these, most Federal rules are commonsense protections of vital freedoms that we cherish as Americans. Freedom from air pollution and water pollution. Freedom from dangerous consumer appliances. Freedom from workplace discrimination and exploitation. Freedom from predatory business practices and monopolies.

Moreover, rules have made our people freer and our country safer, healthier, cleaner, more just, more equitable, and more secure.

Yet President Trump and my GOP colleagues in the House have made destroying government rules one of their top priorities, and they have made of deregulation a mindless political fetish.

But they target only certain kinds of rules. The administration hates rules that get in the way of corporate power. They want to get rid of rules that restrict Wall Street and the finance industry. They want to scrap rules that enforce the Clean Water Act and the Clean Air Act and rules that restrict the freedom of polluters.

They love other kinds of rules. They want rules that interfere with women's rights to make their own healthcare decisions and decisions about birth control and reproduction. Just this past May, the administration issued a gag rule that blocks recipients of Federal family planning funds from counseling or advising women about abortions, and also compelling expensive physical, financial,

and programmatic segregation between units that provide such counseling and those that do not.

They pile rule upon rule in the SNAP program to impose a kind of bureaucratic extremism which makes it impossible for people to access nutritional benefits that they need.

So regulations, like statutes or ordinances or constitutions, are just forms of law. They can be good, they can be bad. They can be efficient, they can be inefficient, fair or not. But my colleagues invite us to believe that Federal regulation is, in general, categorically burdensome and costly. That's false, and we've got a way to show it.

The Office of Management and Budget annually issues a congressionally mandated report that identifies the costs of government rules on the private sector and the estimated financial benefits produced for the American people. Every year this report shows objectively that the economic benefits of Federal rules far outweigh the cost.

Quite shockingly, the administration tried to bury this year's report, releasing it 2 months late, almost certainly because its findings undercut everything the President has stated about government rules.

The report found that last year Federal rules imposed around $5 billion in costs on businesses. At the same time, they resulted in more than $27 billion in benefits to the public. The regulatory benefits to taxpayers are more than five times the cost of these rules.

The costs of an America without any Federal rules are not hard to imagine, but they are impossible to accept. Cars without backup cameras or seatbelts. Peanut butter made in unsanitary conditions. Banks and hedge funds freed from rules of prudential lending. Coal mines that poison coal miners and collapse on human beings with impunity. Predatory payday lenders operating without a CFPB checking them. Out-of-control data breaches. And so on.

This deregulatory project in our economy and environment is risky and dangerous. We cannot risk American lives and our environment because the President wants to reward large campaign donors while using the regulatory bogeyman to try to destroy democratically chosen rules.

Let's think pragmatically and not ideologically. Let's remember that Federal rules are just America's rules. And when it comes to building a strong democracy, laissez isn't fair.

Thank you very much, Mr. Chairman.

Mr. PALMER. I thank the gentleman.

I'm pleased to introduce our witnesses.

Mr. James "Bo" Reese, president of the National Association of State Chief Information Officers, and Chief Information Officer, Office of Management and Enterprise Services, State of Oklahoma.

Mr. John Riggi, senior advisor for cybersecurity and risk for the American Hospital Association.

Mr. Robert Weissman, president of Public Citizen.

Mr. Christopher Feeney, executive vice president of the Bank Policy Institute.

And Mr. Oliver Sherouse, policy analytics lead for the Program for Economic Research on Regulation at the Mercatus Center.

Welcome to you all.

Pursuant to committee rules, all witnesses will be sworn in before they testify. Please stand and raise your right hand.

Do you solemnly swear or affirm the testimony you're about to give is the truth, the whole truth, and nothing but the truth, so help you God?

The record will reflect that all witnesses answered in the affirmative.

Please be seated.

In order to allow time for discussion, please limit your testimony to 5 minutes. And your entire written statement will be made part of the record.

As a reminder, the clock in front of you shows the remaining time during your opening statement. The light will turn yellow when you have 30 seconds left and red when your time is up. Please also remember to press the button to turn your microphones on before speaking.

The chair now recognizes the gentleman, Mr. Reese, for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF JAMES "BO" REESE

Mr. REESE. Thank you, Chairman Palmer and Ranking Member Raskin and members of the subcommittee. Thank you for inviting me to testify before you today on the burden of Federal regulations and their impact to State governments.

My name is Bo Reese, and I serve as the chief information officer, or CIO, for the State of Oklahoma. I also serve as the president of the National Association of State Chief Information Officers, or NASCIO.

All 50 States and three territories are members of NASCIO, and we represent the interests of government-appointed State CIOs who acted as the top IT officials for State government.

Today I would like to provide the subcommittee an overview of how Federal regulations hamper the ability of State CIOs to offer effective and efficient technology and IT services. I will also touch upon how the complex Federal regulatory environment is duplicative in nature, contributes to inconsistent Federal audits, and drives cybersecurity investments based on compliance and not risk, which is the more secure approach.

State CIOs act as the technology and IT provider for State agencies. State agencies administer Federal programs, like Medicaid, SNAP, unemployment insurance, and in so doing exchange data with Federal agencies. Because of this intergovernmental relationship, Federal agencies impose rules on State agencies and all their requirements in audits which then flow to State CIOs who provide IT services to State agencies.

Compliance with the multitude of Federal regulations is burdensome on States, especially those like Oklahoma that have consolidated or unified our IT service delivery. IT unification has resulted in $372 million in cost savings and avoidance for Oklahoma.

Before IT unification, Oklahoma was supporting 129 email servers in State government, 76 different financial systems, 22 time and attendance systems, and 30 data center locations. After the 5-

year IT unification process, we were able to reduce redundancies and leverage economies of scale, further enabling the hundreds of millions in savings and cost avoidance.

The biggest hurdle we faced in achieving IT consolidation was compliance with Federal regulations. Our Federal agency partners are regulating the States not in a streamlined fashion, similar to the way we now operate, but in a siloed way that impedes our ability to operate effectively. States must comb through thousands of pages of Federal regulations to ensure that they are in compliance while administering Federal programs.

And even though many Federal regulations are similar in nature, they each have minor differences, which then requires one-off adjustments for each Federal regulation. This obscures the goal of IT consolidation, which ultimately produces savings for taxpayers.

We certainly understand the importance of regulations and are not advocating their wholesale elimination. The problem is not that there is regulation, but that Federal requirements are organized by Federal individual program and do not follow the industry-recommended approach, which would regulate cyber threats by their risk.

The siloed Federal regulatory approach is carried forward in the Federal audit process. Audits are conducted program by program and not holistically. This means that my office responds to the same audit questions multiple times, again and again, year after year.

For example, in Oklahoma, the IRS audited one State agency multiple times because it viewed different programs as distinct and separate entities. My office had to answer hundreds of questions, attend multiple audit meetings, and deliver additional explanatory material multiple times for one State agency.

This wasteful and inefficient process is repeated time and time again across many different State agencies for each Federal regulatory entity, not to mention the fact that several auditors had different results even though they examined the same audit environment.

A great example of this inefficiency is, in 2016, the State of Oklahoma performed 14 audits over 8 months on the same IT environment. In 2017, we had 11 audits that took us 7 months and all of our resources to perform.

Ultimately, we believe that there is a more efficient and holistic way of ensuring data security and allowing States to implement IT consolidation plans that have proven to generate cost savings.

We would like your assistance in getting Federal regulators to the table with the State CIOs so that we can harmonize regulatory environments and streamline the audit process together.

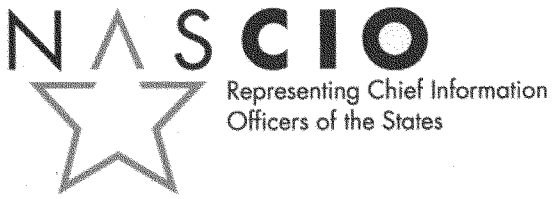
To this end, NASCIO members have already started the process of identifying the differences with two major regulations. And I have a great example of what we've performed already today. The IRS Publication 1075 and the FBI–CJIS are the two that we compared.

We hope to engage with our Federal partners further and appreciate the subcommittee's support in reducing the regulatory burden on States.

In closing, I would like to thank the subcommittee for the opportunity to testify on this important issue, and also like to express our gratitude to Chairman Gowdy for initiating the GAO study on the State impact of Federal regulations in October of last year.

I look forward to your questions, and thank you.

[Prepared statement of Mr. Reese follows:]



Statement before the House Oversight Committee,

Intergovernmental Affairs Subcommittee

"Regulatory Divergence: Failure of the Administrative State"

Testimony of James "Bo" Reese

President, National Association of State Chief Information Officers (NASCIO) & Chief Information Officer, Information Services, Office of Management and Enterprise Services, State of Oklahoma

July 18, 2018

Chairman Palmer, Ranking Member Raskin, and members of the subcommittee, thank you for the opportunity to appear before you to testify on the burden of federal regulations on state government, specifically state IT.

My name is James "Bo" Reese and I serve as the chief information officer (CIO) for the State of Oklahoma. In Oklahoma, I lead Information Services, a division of the Office of Management and Enterprise Services (OMES), with the mission of partnering "with State of Oklahoma agencies and affiliates to deliver quality, cost effective and secure IT services." I also serve as the president of the National Association of State Chief Information Officers (NASCIO) and it is in this capacity that I testify today.

NASCIO is a nonprofit, 501(c)(3) association representing state chief information officers and information technology (IT) executives and managers from the states, territories, and the District of Columbia. State CIOs are governor-appointed, executive branch officials who serve as business leaders and advisors of IT policy and implementation at the state level. All states have a CIO and all CIOs serve the executive branch of state government. The state CIO role takes many forms, some are cabinet officials, some serve under a cabinet secretary, and others are executive directors. Regardless of the title, state CIOs share the common function of setting, implementing, and delivering on the state's IT policy.

During today's hearing, I would like to provide the subcommittee a description of how federal data security regulations impact the effectiveness and efficiency of state IT, state government cybersecurity, and state budgets. I will aim to describe and offer examples of how duplicative, complex, and often conflicting federal regulations and their accompanying audits hinder state governments from achieving a more effective and efficient IT enterprise and cybersecurity posture. I will also discuss possible solutions to reduce the regulatory burden so that we may continue to achieve two major goals, ensuring citizen data security and improving government efficiencies.

Role of the State CIO and the Federal-State Intergovernmental Relationship

State CIOs provide enterprise direction and IT services primarily to the executive branch of state government such as state agencies, commissions, and boards. As the technology leader and IT provider for state government's executive branch, state CIOs aim to manage state IT service and infrastructure as one unified enterprise. State CIOs seek to leverage economies of scale which results in savings for state government and, ultimately, state taxpayers.

In my state, the IT enterprise is unified, which means that state IT employees, assets, and services operate through a centralized model. My office provides IT services for all but one of the state's agencies, commissions, and boards, which number over 100. Many states operate in a centralized fashion, while others are more federated. Regardless of where a state's CIO organization sits on the centralized versus federalized spectrum, all state CIOs provide technology and IT services to state executive branch agencies.

All states administer federal programs like Medicaid, unemployment insurance, Supplemental Nutrition Assistance Program (SNAP), and many others. It is due to this intergovernmental partnership that states become subject to burdensome federal regulations and their accompanying

audits. However, federal data security regulations and accompanying audits have not kept pace with changing state government IT business models and are increasingly hindering the ability of state CIOs to streamline processes and deliver savings to state taxpayers.

State Governments are Unifying Diverse IT Environments for a More Efficient IT Enterprise

One way of boosting efficiencies is through IT consolidation or as we call it in Oklahoma "IT unification." Prior to legislatively mandated IT unification, Oklahoma was supporting seventy-six financial systems, twenty-two time and record keeping systems, seventeen types of document imaging systems, thirty data center locations, and one hundred and nine distinct electronic mail and smart phone services. To address this duplication and reduce inefficiencies, the governor signed the *Information Technology Consolidation and Coordination Act of 2011* which charged my office with improving the efficiency of the state's technology service offerings. As a result of this five-year process, we were able to achieve $372 million in savings and cost avoidance; this number is expected to grow over the coming years.

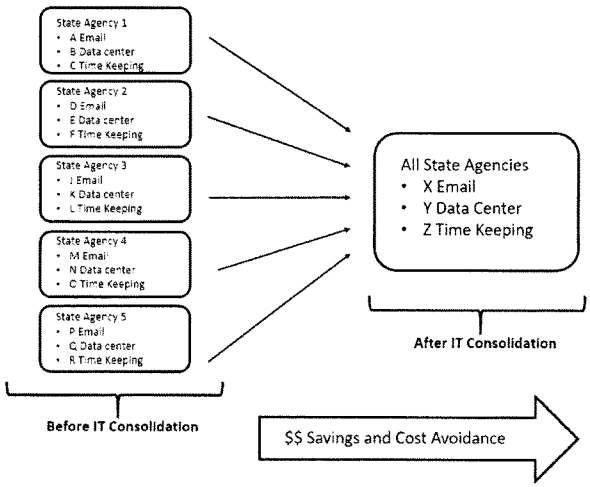


Figure 1: Graphic representation of IT Consolidation/Unification

Oklahoma saw an added benefit through IT consolidation/unification related to cybersecurity. With a centralized and unified IT structure, the state CIO's office became increasingly aware of the security risks and events that were previously buried at the agency level. This gave Oklahoma increased visibility into security events and allowed us to better manage and respond to security threats.

The benefits to IT consolidation/unification are well documented and many states have embarked on this path. In NASCIO's annual Top Ten priorities survey, state IT consolidation has always ranked in the first, second, or third priority among state CIOs (See, NASCIO Top Ten) since 2006. As was the case in Oklahoma, the biggest challenge in achieving the savings and efficiencies associated with IT consolidation/unification was compliance with federal regulations.

Federal Regulations Fail to Recognize Changing State IT Business Models and Impede IT Consolidation/Unification Efforts

State CIOs and the business of state government IT has rapidly adapted to fiscal pressures, changing technologies, and reductions in the state IT workforce. These and other environmental forces have forced state CIOs to seek more effective business models, hence the drive toward IT consolidation/unification. However, federal regulators and auditors fail to recognize the changing technology and IT business models in state government which impedes the ability of states to efficiently and effectively meet their own needs.

Following the passage of Oklahoma's *Technology Consolidation and Coordination Act of 2011*, we developed a five-year IT unification plan that mapped how and when state agencies would transition to the new consolidated/unified IT structure. The most challenging part of this process was not implementing the technology but working with state agencies that erroneously believed or were led to believe that federal regulations would not allow such a transition. Some state agencies held these beliefs due in part to their own interpretations of federal regulations or the interpretations supplied to them by federal auditors and regulators based on past regulatory compliance activity. As a result, we had to devote time and resources working with our state agency customers to explain to them that the unified IT structure could and would meet the compliance expectations of their federal partners. We continue to devote personnel time and resources to meet federal regulatory demands because our federal partners do not recognize our IT service model.

Oklahoma is not the only state that finds the federal regulatory process burdensome and challenging. Many state CIOs and Chief Information Security Officers (CISO) invest an inordinate amount of time identifying duplicative federal regulatory mandates, identifying differences, participating in federal audits, reconciling diverse interpretations of federal regulations, and responding to inconsistent audit findings. In a recent informal survey of state CISOs, some were able to quantify the federal regulatory burden (please see **Attachment 1** for details):

- Oklahoma: 10,712 hours per year with compliance activities and support
- Maine: 11,160 hours spent responding to six federal regulatory agency audits
- Kansas: estimated 14,580 hours every three years managing federal audits and compliance
- Colorado: estimated 2,760 hours per year

(* Note: 40 hours of work per week equates to 2,080 hours of work per year)

The time spent on federal regulatory compliance and audit activity is just one way that the federal regulatory regime impairs the ability of state governments to set and meet their own priorities. Another way federal regulations impede the IT consolidation/unification process is through the "prior approval" and/or "prior notice" requirements. Federal regulations like IRS Publication 1075

require 45-day advance notice (e.g. IRS Publication 1075) when states utilize contractor or contemplate a move to the cloud. Regulations like FBI-CJIS require prior approval of the CJIS systems officer[1] to implement compensating controls (See 5.13.7.2.1 Compensating Controls, FBI-CJIS). These notices and prior approvals have caused delays implementing aggressive IT consolidation/optimization timelines and impede the ability of states to select and deliver technology solutions to state agencies.

These types of federal regulatory requirements hamstring the ability of state CIOs to deliver technology and IT solutions effectively and efficiently to state agency customers and ultimately to state citizens. As the mission statement for OMES states, my first priority as state CIO, like many others, is to deliver quality, cost effective, and secure IT services. However, the increasing federal regulatory burden on state CIOs is forcing state CIOs to prioritize compliance instead of the aforementioned goals. Preliminary data from the 2018 State CIO Survey (to be released in October 2018), shows that 71 percent of state CIO respondents consider "ensure IT systems comply with security and regulatory requirements" as their top priority, followed by "create and drive IT strategy that aligns to overall state objectives" (60 percent), and "improve IT governance" (40 percent). These results further illustrate how the federal regulatory environment is distorting the priority of state CIOs away from quality service delivery.

Federal Data Security Regulations Do Not Enhance the Cybersecurity Posture of States and Does Not Utilize a Risk-Based Approach

Federal data security regulations were designed to guard citizen information and state CIOs are keenly aware of this responsibility. "Security" ranks as the number one priority in the annual NASCIO Top Ten priorities survey and has maintained that position for the past five years. However, compliance activity does not equate to security and often has the opposite effect.

As previously stated, state CIOs aim to operate the state government IT environment as a single unified entity or "enterprise." State CIOs support the mission of state agencies and the federal programs they administer with IT and technology and are rarely, if ever, the direct recipients of federal funds or grants. Because state CIOs deliver enterprise IT services to state agencies that administer federal programs, state CIOs and the larger IT enterprise must also comply with federal regulations that are imposed on those state agencies. Thus, state CIOs find themselves operating in an increasingly complex regulatory environment driven by federal regulations that are promulgated by the federal programmatic agency thinking only of their agency's data rather than embracing a holistic view of data security and organizing by risk which industry standards, including NIST, recognize as the more secure approach.

[1] The CJIS Systems Officer (CSO) is an individual located with thin the CJIS System Agencies (CSA) responsible for the administration of the CJIS network for the CSA. (FBI-CJIS 3.2.2)

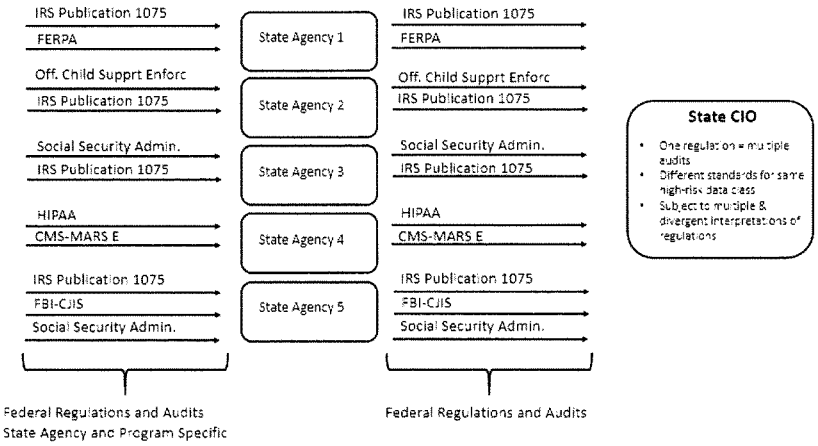


Figure 2: Current state of federal regulatory impact on state CIOs

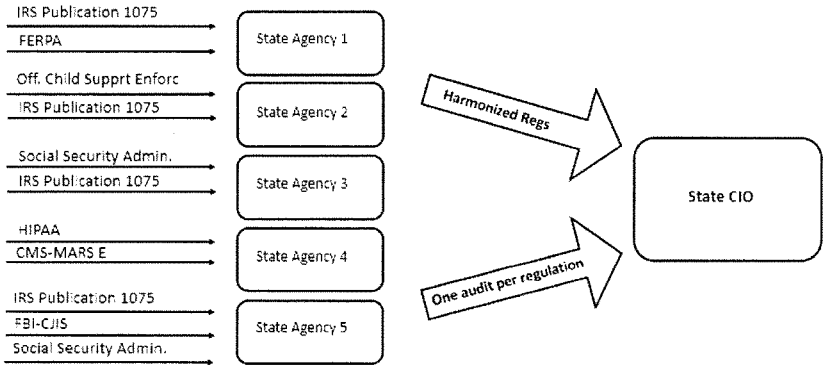


Figure 3: Desired state of federal regulatory compliance and audits

Ninety-five percent of state CIOs reported that they have "adopted a cybersecurity framework based on national standards and guidelines" in the 2017 NASCIO State CIO Survey. NIST standards are widely regarded among state officials as the preeminent resource for approaching cyber risk. The NIST Cybersecurity Framework describes itself as a "risk-based approach to managing cybersecurity risk," (NIST Cybersecurity Framework, page 3) and notes that the benefit of "this risk-based approach enables an organization to gauge the resources needed to achieve cybersecurity goals in a cost-effective, prioritized manner," (NIST Cybersecurity Framework, page 11). Congress, also, spoke to the risk-based approach in the E-Government Act of 2002 (P.L.

107-347). The Act tasked NIST with the development of "standards to be used by all federal agencies to categorize all information and information systems…according to a range of risk levels;" (E-Government Act of 2002, P.L. 107-347, Section 20 (b)(1)(A)). However, even as the federal government attempts to govern its own security methodology as one based on risk, the same approach is not utilized by federal agencies when imposing their regulatory requirements on their state government partners.

Consider this example: most would agree that tax information, criminal justice information, and social security information are high-risk data assets that must be protected at the highest levels of security. However, the Internal Revenue Service (IRS), Federal Bureau of Investigations – Criminal Justice Information Services (FBI-CJIS), and the Social Security Administration (SSA) have three different standards for many aspects of security including the rule that governs unsuccessful login attempts:

Federal Regulation:	IRS Publication 1075	FBI-Criminal Justice Information Services	SSA Electronic Information Exchange Security Requirements and Procedures
Unsuccessful logins	Information system must enforce a limit of 3 consecutive invalid login attempts by a user during a 120 min period, and automatically lock account for at least 15 mins.	Where technically feasible, system shall enforce limit of no more than 5 consecutive invalid attempts, otherwise locking system for 10 mins.	SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information…SSA recommends no fewer than three (3) and no greater than five (5).

As the example above illustrates, federal regulations may speak to the same or similar security topic but are inconsistent in their requirements. Complicating the regulatory environment are the plethora of federal regulations to which state CIOs are subject. Below are some of the federal regulations with which state agencies and thus the state CIO must comply:

- Internal Revenue Service (IRS) Publication 1075
- FBI Criminal Justice Information Services Security Policy (FBI-CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Office of Child Support Enforcement security requirements[2]
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA)
- U.S. Department of Labor - State Quality Service Plan: Agency Assurances
- 42 CFR part 2 - Substance Abuse and Mental Health Services Administration
- Family Educational Rights and Privacy Act (FERPA)

[2] 45 CFR §307.5 Mandatory computerized support enforcement systems.

- Gramm Leach Bliley Act
- Child Internet Protection Act of 2000
- Child Online Privacy Protection Rule of 2000

Federal Regulatory Audits are Repetitive and Inconsistent

Compliance with numerous federal regulations and the diversity of their requirements are only part of the regulatory burden faced by states. Federal regulatory audits are conducted on a regular basis, usually every two or three years. Despite the multi-year gap between formal audits, states expend precious time and resources preparing for federal audits, responding to audit findings/corrective actions reports and reconciling divergent interpretations from individual auditors.

The audit process itself is inefficient because the state is audited not as one entity, but by program. David Carter, the CISO for Kentucky explains it this way:

> "We have three agencies (Cabinet for Health and Family Services, Department of Juvenile Justice, and Department of Workforce Investment) that receive Social Security Administration (SSA) data, four that receive IRS data (the three mentioned plus the Department of Revenue). This is for the most part all the same data, but is distributed under seven unique need and use agreements. As such, we have seven agency level audits for each need and use agreement and one additional specific to IT as the state transmission center (STC) for a total of eight audits for common data, all operating under the same controls and infrastructure.
>
> For the Commonwealth, the core challenge that we encounter is the overlap between all audit and attestation processes related to federal compliance. Even having established responses that can be recycled over and across these audits take considerable time and resources. As an example, we are audited across four agencies for the IRS and three for the SSA. This is single source data from a common federal repository. Where one compliance review would suffice, I have to respond seven. Adding these to the other requirements within our environment, we respond to 23 to 26 audits annually diverting resources, time, and investment from matters that provide meaningful risk reduction across our infrastructure as a whole." (Senate Homeland Security and Governmental Affairs testimony attachment, June 2017).

Further, federal audits results or "findings" can also be inconsistent even though auditors are examining one IT policy. Louisiana's CISO, Dustin Glover, stated: "A clear example of the significant inconsistencies we face with federal audits/assessments/reviews is illustrated in our most recent onsite IRS assessment performed January 2017. Five Louisiana state agencies were assessed by five separate IRS assessors **all auditing the same exact statewide Information Security Policy** with the following breaking down of findings:

	Findings
Agency =1	**32**
Agency =2	**27**
Agency =3	**23**
Agency =4	**14**
Agency =5	**11**

Figure 4: Inconsistent audit findings

As you can see, consistency is lacking and the agencies were audited with the same exact federal regulation." (Senate Homeland Security and Governmental Affairs testimony attachment, June 2017).

Solutions for a More Harmonized Federal Regulatory Environment and Normalized Audit Practice

State governments are acutely aware of the responsibility to secure citizen data which is why state CIOs make every effort to comply with the federal rules and regulations that govern the use of federal data assets. However, State CIOs believe that there is a more effective way to ensure security and decrease the regulatory burden. We would like to propose that our federal regulatory partners work collaboratively with state CIOs to harmonize disparate regulations and normalize the audit process. We have begun the conversation with several federal regulatory agencies and have sought the assistance of the Office of Information and Regulatory Affairs within the Office of Management and Budget. We have also received support for our effort from the National Governors Association (NGA).

We would like to offer several possible solutions including:

- Through legislation, Congress should form a working group or committee comprised of federal regulators and state CIOs to identify regulatory disparities and harmonize regulatory requirements.
- To improve the audit process, federal regulators should be required to communicate their audit priorities and results not just to the programmatic agencies but also to all affected stakeholders, including state CIOs.
- Federal regulatory audits should be conducted once for multiple programs instead of being conducted multiple times for each program or each use of federal data.
- Compensating controls that are acceptable to federal regulators should be shared with a broad audience, instead of being limited to the affected state agency or program.

NASCIO has started the process of identifying inconsistencies with two major federal regulations, IRS Publication 1075 and FBI-CJIS. We would like to continue with this work in collaboration with our federal regulators to address additional regulations.

Thank you for your attention on this issue and inviting me to share the perspective of state CIOs. We look forward to working with the House Intergovernmental Subcommittee and Oversight Committee members to reduce the regulatory burden on states.

NASCIO

Attachment 1: Federal Regulatory Burden on States

Question 1: How much does it cost states to comply with federal regulatory and data security requirements? Can you give examples of how state budgets are impacted? How many hours are state officials spending to comply with these requirements?

OKLAHOMA

There are the quantitative costs:
All IT contracts, projects, and central IT services have a regulatory "filter" that is staffed by my office. We review any and all IT contracts that have impact to any level of PII or above. If it is potentially regulated data that could be impacted (hardware, software, services, etc.) we review, provide the assessment, changes to terms, and compliance review prior to implementation. We also oversee the implementation to make sure we have in the final product at the required level of compliance.

This includes performing safeguard computer security evaluation matrix (SCSEM), contract languages, training, background checks, auditing of security practices and vendor compliance to state and federal regulations (this slows the state down, even though we have streamlined this process to make is as efficient as possible).

Added costs to procurement: the added complexity in the state procurement processes for vendors to supply hardware or services that meet SCSEM or Regulatory specifications have an upcharge for these added requirements from vendors.

Added costs in timeframes: the ability to make strategic investments in IT and Security with agencies that have these regulatory environments takes much longer due to the complexities in architecting the solutions, allowing for the time for assessment for compliance, the processes to seek permission or notify the regulatory entity before the state can commit; and then the added complexity to re-submit state security plans with the changes back to the regulators.

The quantifiable costs:
I did a high-level review of the number of security staff that are involved in activities for federal compliance. We answered the question of "What is the average of the time spent over a year" working on issues related to federal regulation, audit, and compliance work. I took those average estimates as a percentage of time against people's salaries. We estimate that federal compliance costs the security group $447,138.70 in the security area alone. This is made up of the following staff time assessments and estimations:

- 2 Audit Staff - (60% respectively) - 1248 hours each
- 1 Security Architect - (35%) -728 hours
- 6 Security Engineers (placed at Regulatory Agencies - Average 40%) - 4,992 hours total
- Security Director - (40%) - 832 hours
- State CISO and Deputy CISO - (40% respectively) - 832 hours each

This equates to a combined hourly impact based on the 2,080 workable hours a year to ballpark to around **10,712 hours a year** spent with compliance activities and support.

Following these estimates of these 12 resources on 2,080 workable hours a year creates a total of **24,960** hours as a team available to the state to achieve our state cyber mission, with nearly 10,712 hours spent equates to around **43%** of the total time spent on compliance activities and support as a whole.

That doesn't factor in the other 730 IT staff that have to work with my staff to achieve compliance activities, it also doesn't account for the agency staff that we have to interface with that have dedicated people for program compliance etc.

Specific findings to prevent access from personal computers to state systems with regulated data; was highly disputed as the state provide a VPN into a Virtual Desktop System that then connected to a user's PC to allow remote access. The state was not able to allow for this incidental emergency access and was forced to procure laptops for every agency program staff member and IT to have a state asset to close this critical finding.

MAINE

The State of Maine regulatory landscape includes 6 Federal agencies.

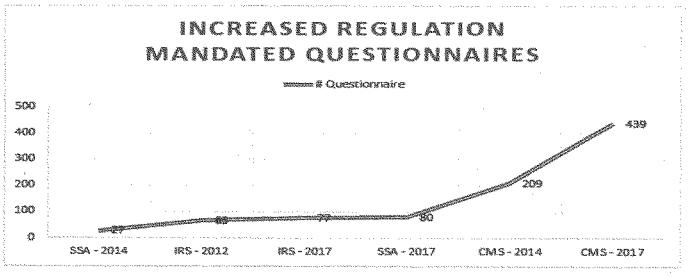
1. The State must analyze over 1,000 pages of Federal audit questionnaire.
2. The single source document for almost all the questions/mandates is the National Institute of Standards and Technology (NIST) Security Controls.

#	Regulatory Agency	State Resources	Total Hours
1	Internal Revenue Service (IRS)	12+	4,000
2	Social Security Administration (SSA)	4+	2,500
3	U.S. Treasury	1	60
4	Health Portability and Accountability Act (HIPAA)	6+	800
5	Criminal Justice Information Service (CJIS)	3+	800
6	Centers for Medicare and Medicaid Services (CMS)	12+	3,000
Total			11,160

Published Regulatory Mandate Documents	
Federal Regulatory Publication	# of pages
IRS Publication 1075	180
SSA TSSR	85
U.S. Treasury (NIST SP 800-47 & FISMA)	74
HIPAA (Security Rule, plus 6 additional documents)	155
Centers for Medicare and Medicaid Services CMS) (Harmonized Security and Privacy Framework, Minimum Acceptable Risk Standards, Catalog of Security and Privacy Controls, AE ACA SSP)	534
Total	1028

Historical Overview of Increasing Regulations:

This graph plots the growth in the number of questions over the last 3 years.



Examples of Duplicate Reports:

Often, the same report must be filed with the same regulatory agency, but on behalf of different State agencies, and sometimes, bureaus within the same agency. For instance, DHHS-DSER, DHHS-OFI, DOL, and MRS

all have to file the very same report with the Internal Revenue Service. Maine is spending hundreds of hours reviewing and completing such duplicate reports.

Example of Duplicated Regulatory Deliverables		
Federal Agency	**#**	**Regulatory Deliverable**
Internal Revenue Service	4	Safeguard Security Reports
	4	Corrective Action Plans
SSA	4	Compliance Review Questionnaires

Examples of Duplicated Questions Worded Differently:

#	Internal Revenue Service	Social Security Administration
1	Describe how the agency maintains and disseminates to designated agency officials: A) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.	Does the agency have a published password policy for user of systems and/or applications that receives, processes and stores Social Security provided information?
2	Describe how the agency manages information system authenticators (or passwords). Describe how the agency implements the following authenticator requirements: A) Enforces non-privileged account passwords to be changed at least every 90 days. B) Enforces privileged account passwords to be changed at least every 60 days. C) Prohibits password reuse for 24 generations.	Does the security software package impose and enforce limitations on password repetition (i.e., will not permit usage of the same password within a specified number of password expiration cycles?

Suggested approach to the issue (reduce the over-11,000 person-hours required to complete the audits today):

1. Required reporting for the six Federal agencies could be consolidated and streamlined for similar topics: Ask the question once; Not six times, in slightly different language.
2. Federal agencies could agree on a standardized reporting mechanism that satisfies the needs of all the Federal Agency stakeholders.
3. In addition to the standardized questions, there could be a sub-section in which each Federal agency could ask their specific questions.

The state budget makes a fixed allocation for I.T. Which means, the higher the federal regulatory burden, the lower the investment in other business-critical I.T. activities.

PENNSYLVANIA

In Pennsylvania there are three IT delivery centers with federal requirements related to Social Security Administration (SSA) regulations, IRS Publication 1075, and FBI-CJIS.

Some federal requirements provide partial funding, so those requirements can be supported and completed in timely manner. Federal requirements that are made without funding can be burdensome since budgets are very tight and often not enough time is allotted to the budget plan.

The question regarding how many hours are spent on compliance is too general to provide a clear answer as we have no dedicated staff working specifically on federal requirements. Almost all security work performed benefits the entire organization by aligning with a Cybersecurity Framework which helps meet federal compliance requirements. Regarding SSA, we spend on average 20-30 hours just preparing annually for an estimated personnel cost $23,400 to prepare for the SSA audit.

Costs increase from there. Cost of security log correlations and custom alerting could potentially equate to around 100 hours of a senior engineer, along with integration costs for vendor engineers to initially setup.

For Pennsylvania's Departments of Revenue, Labor and Industry, Insurance, State and Banking and Securities, the estimated cost to comply with federal regulatory and data security requirements is: $2,492,278. Budgets are impacted by the aforementioned costs which are essentially unfunded mandates by the IRS.

KANSAS

The State of Kansas estimates that every three years, it spends approximately 14,580 hours managing federal audits and compliance. These hours include information security resources, technical resources, and also program management. The estimated cost is approximately $660,600.00 over the course of three years. This does not include any major capital expenses to procure new equipment or software to achieve compliance such multi factor authentication, FIPS compliant VPN solutions, etc. A majority of the time and resources are spent with addressing IRS FTI and FBI CJIS requirements. As the state modernizes and moves towards hosted solutions, the hours and costs for meeting compliance are expected to rise.

Federal Regulators: IRS									
		Audit Preparation	Audit	Corrective Action Plan Response	Safeguard Security Report (SSR)	Internal Inspections/ Site Visits	Sum	Rate	Cost
KS Dept of Children and Families (Two programs)	Information security office	80	40	120	80	80	400	60	$24,000
	Technical resources	40	40	160	10	0	250	50	$12,500
	Program management	80	160	160	80	80	560	40	$24,400
KS Dept of Revenue	Information security office	40	40	80	40	80	280	60	$16,800
	Technical resources	20	40	120	10	0	190	50	$9,500
	Program management	40	80	80	40	80	320	40	$12,800
KS Dept of Labor	Information security office	40	40	80	40	10	210	60	$12,600
	Technical resources	20	40	120	10	0	190	50	$9,500
	Program management	40	80	80	40	10	250	40	$10,000
						Total Hours	2650	Total Cost	$130,100
Federal Regulators: SSA									

		Audit Preparation	Audit	Corrective Action Plan Response	TSSR/ SEQ	Internal Inspections/ Site Visits	Sum	Rate	Cost
KS Dept of Children and Families	Information security office	40	40	40	40	80	240	60	$14,400
	Technical resources	20	20	40	10	0	90	50	$4,500
	Program management	80	80	80	40	80	360	40	$14,400
KS Dept of Revenue	Information security office	20	20	40	20	80	180	60	$10,800
	Technical resources	20	20	40	10	0	90	50	$4,500
	Program management	40	80	40	20	160	340	40	$13,600
KS Dept of Labor	Information security office	20	20	40	20	80	180	60	$10,800
	Technical resources	20	20	40	10	0	90	50	$4,500
	Program management	40	80	40	20	160	340	40	$13,600
KS Dept of Health and Environment	Information security office	40	40	40	40	80	240	60	$14,400
	Technical resources	20	20	40	10	0	90	50	$4,500
	Program management	80	80	80	40	80	360	40	$14,400
						Total Hours	2600	Total Cost	$124,400
Federal Regulators: CMS									
KS Dept Aging and Disability Services		Audit Preparation	Audit	Corrective Action Plan Response	Agency Questionnaire	Internal Inspections/ Site Visits	Sum	Rate	Cost
	Information security office	40	40	40	40	80	240	60	$14,400
	Technical resources	20	20	40	10	0	90	50	$4,500
	Program management	80	80	80	40	80	360	40	$14,400
KS Dept of Health and Environment	Information security office	40	40	40	40	80	240	60	$14,400
	Technical resources	20	20	40	10	0	90	50	$4,500
	Program management	80	80	80	40	80	360	40	$14,400

						Total Hours	1380	Total Cost	$66,600
Federal Regulators: FBI-CJIS									
KS Highway Patrol		Audit Preparation	Audit	Corrective Action Plan Response	CJIS Questionnaire	Internal Inspections/ Site Visits	Sum	Rate	Cost
	Information security office	40	40	40	40	0	160	60	$9,600
	Technical resources	20	40	120	10	0	190	50	$9,500
	Program management	40	80	60	40	5400	5620	40	$224,800
KS Bureau of Investigation	Information security office	40	40	40	40	0	160	60	$9,600
	Technical resources	20	40	120	10	0	190	50	$9,500
	Program management	40	80	60	40	0	220	40	$8,800
KS Dept of Corrections	Information security office	40	40	40	40	80	240	60	$14,400
	Technical resources	20	40	120	10	0	190	50	$9,500
	Program management	40	80	60	40	80	300	40	$12,000
						Total Hours	7270	Total Cost	$307,700
Federal Regulators: HHS/OCSE (NDNH)									
		Audit Preparation	Audit	Corrective Action Plan Response	HHS (NDNH) Questionnaire	Internal Inspections/ Site Visits	Sum	Rate	Cost
KS Dept of Children and Families	Information security office	20	20	20	20	0	80	60	$4,800
	Technical resources	20	20	20	10	0	70	50	$3,500
	Program management	40	40	40	20	10	150	40	$6,000
KS Dept of Labor	Information security office	20	20	20	20	0	80	60	$4,800
	Technical resources	20	20	20	10	0	70	50	$3,500
	Program management	80	80	40	20	10	230	40	$9,300
						Total Hours	680		$31,800
Overall total hours for 3-year period: 14,580 hours									
Overall Total Costs over 3-year period: $660,600 (does not include capital expenses to ensure compliance)									

COLORADO

IRS Publication 1075 Compliance:

In 2017, Colorado was successful in justifying a budget amendment to increase our cybersecurity budget by almost 30%, to build out our Risk and Compliance team. This team facilitates IT audits for all executive branch agencies of state government and conducts risk analysis. We justified and hired 5 FTE's and implemented a Governance, Risk and Compliance (GRC) toolset, in order to track the various controls, audits, findings, and remediation status, for all of the various audits encountered throughout our state agencies.

Colorado is a consolidated state, in which the Governor's Office of Information Technology (OIT) provides IT services and Security (and IT risk/compliance functions) for 17 executive branch agencies.

We have created the chart below, to depict our annual **IRS compliance effort**, and the work associated with this effort. This depicts four Risk and Compliance FTEs who are assigned to four agencies (in scope for IRS Publication 1075) broken down on average hours per week and per month for the three-month periods of January - March and June - August. This is the timeframe in which we prepare and submit the Corrective Action Plan (CAP) and Safeguard Security Report (SSR) to the IRS. During these peak months each analyst (4) averages 3 hours of weekly meetings. This represents a weekly total of 12 hours per week; extrapolated to a month it equals approximately 48 hours each month. Extrapolated to a quarter, it represents 144 hours, during those peak quarters. For the non-peak times (the other 6 months of the year) activities drop down to 25% (of the peak performance) to total 360 overall man-hours for meetings. Additionally, each analyst spends about 4 hours a day X 5 days a (20) week during peak times updating spreadsheets, reading through e-mails, gathering artifacts, helping SMEs to compose narratives.

IRS Pub 1075 Compliance "Risk and Compliance" Resources Only	Analysts/ Agencies assigned	Avg. hours Per Week	Meetings & Activities Per Week	Peak 6-Mo. Total Jan - June	Non-peak month total for other 6 months	Total Man-hours Per Year
Meetings	4	3	12	288	72	360
Tracking	4	20	80	1,920	480	2400
						2760

Note: This chart only includes our "Risk and Compliance" team's hours. This does not include other OIT resources (producing evidence, updating status on recommendations, etc.), and it also does not include personnel representing the agencies. In order to include those resources, it might be prudent to multiply by 2.5 times (2760 * 2.5) which would be ***approximately 6900 hours per year for IRS compliance alone***. This is likely a very conservative estimate!

MARS-E 2 Compliance:

MARS-E 2 compliance requires 2 dedicated FTEs within the Governor's Office of Information Technology. In addition, the agency has at least .5 FTE. This represents approximately 5000 hours per year, maintaining MARS-E 2 compliance.

In addition to the 2.5 FTEs, MARS-E 2 compliance costs another $200,000 to $300,000 annually, this is comprised of:

- Vendors/consultants to help remediate control gaps by recommending, designing, and/or implementing solutions
- Tools/solutions implemented to address control gaps
- Annual control assessments

- Penetration tests
- Vendor internal costs: security FTEs, maintaining documentation, demonstrating compliance, participating in audits, remediating control gaps, etc.

Question 2: Is the federal compliance process incompatible with states that have a consolidated information technology (IT) structure? If so, please explain and provide examples.

TEXAS

The federal compliance process, when leveraging the Risk Management Framework (RMF) developed by the National Institute of Standards and Technologies (NIST), works very well in a consolidated information technology (IT) structure as long as the State has also adopted the RMF as the State's standardized security framework. For States that have not translated their security requirements into the standard RMF format demonstrating compliance with RMF is a challenge and increases costs due to the need to translate existing requirements into the federal standard. Additionally, **several Federal agencies do not leverage the standardized NIST RMF format creating additional difficulties demonstrating compliance due to non-standard frameworks being introduced.**

OKLAHOMA

Not necessarily. The compliance standards should be applied to state programs. The issues is that **few regulators recognize the State CIO and CISO as a formal role in their process.** We need inclusion and we need the ability to engage and help make decisions for the state with our agencies and regulators without having continual roadblocks; regulators should recognize the state CIO authority in these matters.

States need the ability to also have a voice on how these regulations are identified and applied to the state programs. The inconsistency in how the regulations are applied to states such as password length or complexity prevents having a fully consolidated IT infrastructure. Federal regulators continually mandate that states implement the most stringent controls or requirements, which increase costs across the board to all the agencies in the consolidated environment.

MAINE

It doesn't have to be incompatible. All it requires is a well-defined portfolio of MOU & SLA between the state agency and the state's centralized I.T. office. The trickiest one is CJIS, but, even that can be handled. In fact, Maine has already handled the entire federal regulatory framework (in partnership with state agencies), and Maine has had centralized I.T. since 2005. While Maine has worked with its state agencies, the ultimate problem of disparate and conflicting federal regulations, remains.

PENNSYLVANIA

I would not say it's incompatible, it's more of a learning curve with areas to improve upon.

KANSAS

The federal compliance process itself works well with states that have consolidated IT structures. The real issues arise with compliance itself. Many of the compliance requirements aren't compatible with the direction IT is heading as a whole, moving to cloud or vendor hosted IT infrastructures. For example, the IRS still struggles in allowing states to disclose/store "benefits data" with contractors. There are inconsistencies in answers depending on who you ask at the IRS. This greatly impedes states from being able to follow the same IT modernization path that private industry is taking.

COLORADO

It is not incompatible, but it is challenging in that the agencies own the relationships with the federal partners, and Colorado's Office of Information Technology (OIT) is not able to contact the federal partner directly.

For IRS, the agencies are required to submit (for IRS), every 6 months, their CAP and/or SSR. The process is complicated, and the agency-personnel submitting are not technical experts. OIT is not allowed to have an IRS account, from which to submit these documents. We have the technical expertise, but not the IRS access, the agency has the IRS access, but does not have the technical expertise. This results in delays and other inefficiencies.

Similarly, questions to CMS, related to MARS-E 2 or OIT's role as a "Connecting Entity" have to be funneled through the agency - as OIT does not have a direct relationship with CMS.

Question 3: How do communication issues, or a lack of communication, with federal partners hinder or exacerbate these problems with the compliance process?

TEXAS

The greatest hindrances between State and Federal communication are:

a. Many federal agencies' security requirements have not been adopted to the NIST RMF language for their security requirements catalogs. This increases the challenges to merge the disparate and sometimes conflicting federal requirements. Federal Agencies that produce security compliance / control catalogs that are not in the NIST RMF format include:
    1. Centers for Disease Control
    2. Social Security Administration
    3. FBI-CJIS
    4. Department of Health and Human Services
b. It is often unclear in federal Interconnection Security Agreements and contracts exactly which systems are required to comply with Federal law. The difficulties clarifying these requirements can lead to State agencies and the vendors that support them misapplying security requirements, either not fully meeting Federal compliance requirements or applying more security than they are legally obligated to.
c. Another hindrance is that various federal agencies differ on their security control and assessment processes requirements. Whereas, a system that must be compliant with both CMS and HIPAA, becomes a complex task.

OKLAHOMA

While this is greatly improving, state CIO and CISO's have been largely at the mercy of the state agencies' ability to contact regulators and provide us the ability to speak to them to get clarification or direct dialogue, as the regulators do not recognize the state CIO's authority or role in their engagements / contracting processes.

The inability for the federal regulatory entities to have internal dialogue with each other prevents the regulators and states to reach some common-sense approaches to mitigations for compliance and cyber issues.

The federally required NIST 800-53 control framework for Federal Entities is the baseline by which we are working; it would make sense to have some level of review for the controls outlined in federal regulations that baseline back to NIST and an oversight body to identify how those may conflict.

Audit entities for federal regulators should have the ability to collaborate and share audit information. While different standards look at different programs, there should be standardization that would allow for Federal Entities to achieve ways to collaborate, shar information, and achieve their goals for audit and inspection with less duplication of effort on their part and on the part of the states.

MAINE

The ultimate ask would be for any/all federal regulatory compliance to start w/ a baseline response to the NIST 800-53 controls, and then just track the specific delta for a particular compliance rule.

PENNSYLVANIA

In general, communications from federal agencies are highly inconsistent. For example, this year's SSA audit included unannounced cloud controls. All of the communications were scattered via a multitude of emails without a single source like a content management system to house and audit updates as they happened.

Some federal entities only communicate when they feel there's a major issue. Federal entities are also very inconsistent on how frequent they communicate. There is one federal agency that we speak with on monthly calls, while another you only hear from every three years. The increasing security requirements are making the exchange of federal data with state agencies more difficult to implement and support.

KANSAS

Several of the Federal Partners to not have a real large compliance group. This leaves the agency with very few contacts when questions arise. The individuals are constantly out of the office performing site assessments of other states and local governments. Additionally, some requirements are not published for easy accessibility. You must contact the federal partners and have them send you the requirements. This makes it incredibly hard to keep track of changes in requirements. Additionally, a lack of completely consistent controls across all entities following a similar format allows for inconsistency among requirements when most all of the data is at the same MODERATE level.

COLORADO

Questions have to be funneled through the agency, which means that information is often incomplete, unavailable, distorted, or delayed.

Question 4: What are some ways the federal-state compliance process affects cybersecurity?

TEXAS

Security compliance requirements are the primary requirements considered when determining what security measures to put in place to protect an Agency and its information systems. The additional federal compliance requirements play a critical role in prioritization discussion concerning what specific security technologies or services should be invested in, including:

- Whether a cloud provider can be leveraged. Often, due to federal requirements, cloud providers are either not used or the more expensive FedRAMP options are the only viable options.
- Which data centers can be utilized.
- Encryption requirements, both within data centers, cloud environments, and on individual devices, whether at rest or when the data is being transmitted.

OKLAHOMA

The above resources burden has impacts on our ability to be responsive to the needs of the state and the vastly fluid environment of cybersecurity and the threats manifested to us as states.

The compliance-based approach to investments and management of security often is in conflict with the Risk based approach. The states are on limited budgets and have to make decisions that could drastically impact the security posture of the state. In doing so we have to make some risk balanced decisions that could result in a critical finding with a regulator. Those finding come with direct threats to withhold data, that severely impact the states funding, capabilities, and the ability to deliver services to citizens lives, causing states to scramble and make investments on compliance and defund or hold other investments.

MAINE

A compliance framework is different from a risk-based investment strategy. So, while there does exist considerable overlap between federal-state compliance and cybersecurity, there still exists substantial delta between the two. At the end of the day, the fiduciary duty of a state CISO is to pursue the risk-based cybersecurity investment strategy and not one based on compliance.

PENNSYLVANIA

Federal regulations provide guidelines on how best to mitigate risk by following accepted standards. Federal compliance can help encourage senior management support sound cybersecurity practices. The one concern or issue that would help is that federal compliance needs to align with NIST standards as new risks evolve.

Additionally, it should be noted that federal requirements frequently create unfunded expenses to the states, which puts a strain on budgets to meet compliance requirements.

KANSAS

The federal-state compliance process has both positive and negative effects. Following a common RMF allows for streamlining a RMF process within the state. Additionally, audit results assist in advancing and addressing some cybersecurity risks by allocating additional resources or additional system hardening etc. However, going through the compliance nuances multiple times takes away from staffs' time to focus on other areas of cybersecurity, cyber security operations, and advancing the cybersecurity program.

COLORADO

We were not able to use the IRS audit and findings, and other documentation for a Social Security Administration audit of the same systems. This meant that some of the work was done twice, issues are tracked twice and separately. We spend so much time tracking the same issues (but in different formats, same findings across multiple agencies, and for different audits), the time could be better spent in remediation, rather than tracking.

November 6, 2017

Mick Mulvaney
Director
Office of Management and Budget (OMB)
725 17th Street, NW,
Washington, DC 20503

Dear Director Mulvaney,

On behalf of the Nation's Governors and state chief information officers, we write to ask that the Office of Management and Budget's Office of Information and Regulatory Affairs (OIRA) engage with us to harmonize disparate federal cybersecurity regulations and normalize the federal audit process.

Federal cybersecurity regulations can hamper state CIO initiatives like IT consolidation which has shown to produce million in savings for state governments and our taxpayers. Additionally, state governments must utilize scarce cybersecurity professionals with the business of federal compliance instead of investing that same time in security actions that would enhance the cybersecurity posture of the state.

On June 21, the Senate Homeland Security and Governmental Affairs Committee (HSGAC) held a hearing, "Cybersecurity Regulation Harmonization" during which NASCIO vice president and Oklahoma CIO, James "Bo" Reese, spoke about the benefits of IT consolidation and the $286 million in savings reaped for the state through this effort. State CIOs across the country are similarly involved in state IT consolidation/optimization efforts. State CIOs aim to operate the state government IT environment as a unified, single entity or "enterprise." In doing so, they must comply with a wide range of federal cybersecurity regulations that are imposed on individual state agencies. State IT consolidation efforts are hampered by the disjointed nature with which federal cybersecurity regulations were promulgated.

For example, the state government IT environment must reflect compliance with:

- Internal Revenue Service (IRS) Publication 1075
- FBI Criminal Justice Information Services Security Policy (FBI-CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Office of Child Support Enforcement security requirements
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)

- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA)
- U.S. Department of Labor - State Quality Service Plan: Agency Assurances
- Substance Abuse and Mental Health Services Administration (42 CFR part 2)
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act
- Child Internet Protection Act of 2000
- Child Online Privacy Protection Rule of 2000

As stewards of citizen data, we understand and appreciate the need to secure sensitive information. However, the plethora of federal regulations can and have impeded state efforts to produce cost savings for taxpayers and diverts the attention of scarce state government cybersecurity professionals to compliance activities rather than implementing forward-leaning security policies.

We respectfully ask that your office engage appropriate federal agencies, including those that promulgate regulations and audit state government IT, and work with our representative organizations, the National Governors Association (NGA) and the National Association of State Chief Information Officers (NASCIO), to find a solution that satisfies the security and privacy concerns of federal agencies while being cognizant of the cost-saving initiatives and cybersecurity workforce challenges within state government.

We would appreciate your attention, direction, and cooperation in this matter to optimize taxpayer resources while safely securing citizen information.

If you have any questions, please reach out to NGA Legislative Director Mary Catherine Ott (mcott@NGA.org) or NASCIO Director of Government Affairs Yejin Cooke (ycooke@NASCIO.org) for more information.

Sincerely,

Governor Mark Dayton
Chair
Homeland Security and Public Safety Committee

Governor Eric Greitens
Vice-Chair
Homeland Security and Public Safety Committee

Thomas Baden
Commissioner and Chief Information Officer
MN.IT Services
State of Minnesota

Rich Kliethermes
Acting Chief Information Officer
Office of Administration, Information
Technology Services Division
State of Missouri

Mr. PALMER. I thank the gentleman.

The chair now recognizes Mr. Riggi for his testimony.

STATEMENT OF JOHN RIGGI

Mr. RIGGI. Good afternoon. My name is John Riggi, and I appreciate the opportunity to testify on behalf of the American Hospital Association today.

Every day hospitals and health systems confront the daunting task of complying with a growing number of Federal regulations. While Federal regulation is necessary to ensure that healthcare patients receive safe, high quality care, in recent years, clinical staff—doctors, nurses, and caregivers—find themselves devoting more time to regulatory compliance, taking them away from patient care. Some of these rules do not improve care, and all of them raise costs.

Last fall, the AHA issued a report entitled "Regulatory Overload," and I appreciate the opportunity today to discuss the findings. The major findings include that health systems, hospitals, and post-acute care providers must comply with 629 discrete regulatory requirements across nine domains.

The four agencies that promulgated these requirements—the Centers for Medicare and Medicaid Services, CMS; the Office of the Inspector General, Office for Civil Rights, OIG OCR; and the Office of the National Coordinator for Health Information Technology, ONC—are the primary drivers of Federal regulation impacting these providers.

However, providers also are subject to regulation from other Federal and State entities which are not accounted for in this report.

Health systems, hospitals, and post-acute care providers spend nearly $39 billion a year solely on the administrative activities related to regulatory compliance in the nine domains discussed in the report.

An average-sized community hospital of 161 beds spends nearly $7.6 million annually on administrative activities to support compliance with the reviewed Federal regulations. That figure rises to $9 million for those hospitals with post-acute care beds.

Nationally, this equates to $38.6 billion each year to comply with the administrative aspects of regulatory compliance in just these nine domains.

Looked at in another way, regulatory burden costs $1,200 every time a patient is admitted to a hospital.

An average-sized hospital dedicates 59 full-time equivalent employees to regulatory compliance, over one-quarter of which are doctors, nurses, and pulling clinical staff away from patient care responsibilities.

The frequency and pace of regulatory change make compliance challenging and often results in duplication of efforts in substantial amounts of clinician time away from patient care. As new or updated regulations are issued, a provider must quickly mobilize clinical and nonclinical resources to decipher the regulations and then redesign, test, implement, and communicate new processes throughout the organization.

Providers dedicate the largest proportion of resources to documenting conditions of participation, CoPs, adherence, billing and

coverage verification processes. Meaningful use has spurred provider investment in IT systems, but exorbitant costs and ongoing interoperability issues remain. Quality reporting requirements are often duplicative and have inefficient reporting processes, particularly for providers participating in value-based purchasing models.

Again, this creates inefficiency and consumes significant financial resources and clinician staff.

Fraud and abuse laws are outdated and have not evolved to support new models of care. The Stark Law and the Anti-Kickback Statute, AKS, can be impediments to transforming care delivery.

While CMS has waived certain fraud and abuse laws for providers participating in various demonstration projects, those who receive a waiver generally cannot apply it beyond the specific demonstration or model.

The lack of protections extending care innovations to other Medicare or Medicaid patients and commercially insured beneficiaries minimize efficiencies and cost savings realized through these types of models and demonstration projects.

A reduction in administrative burden would enable providers to focus on patients, not paperwork, and reinvest resources in improving care, improving health, and reducing costs.

We have several general recommendations to reduce administrative requirements without compromising patient outcomes:

Regulatory requirements should be better aligned and consistently applied within and across Federal agencies and programs and subject to routine review for effectiveness to ensure the benefit for the public good outweigh additional compliance burdens;

Regulators should provide clear, concise guidance and reasonable timelines for the implementation of new rules;

Conditions of participation should be evidence-based, aligned with other laws, industry standards, and flexible in order to support different patient populations and communities;

Federal agencies should accelerate the transition to automation of administrative transactions, such as prior authorization;

Meaningful use requirements should be streamlined and should be increasingly focused on interoperability and cybersecurity risk considerations without holding providers responsible for the action of others;

Quality reporting requirements should be thoroughly evaluated across all programs to better determine what measures provide meaningful and actionable information for patients and providers and regulators;

Post-acute care rules should be reviewed and simplified to remove or update antiquated, redundant, and unnecessary rules;

With new deliver system and payment reforms emerging, Congress, CMS, and the OIG should revisit the Stark Law and AKS to ensure that statutes provide the flexibility necessary to support the provision of high quality care.

Thank you for the opportunity to provide an overview of AHA's view on regulatory burden. We appreciate the committee's focus on this topic. And I look forward to your questions.

[Prepared statement of Mr. Riggi follows:]

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

Testimony

of the

American Hospital Association

before the

Subcommittee on Intergovernmental Affairs

of the

Committee on Oversight and Government Reform

of the

U.S. House of Representatives

July 18, 2018

Good afternoon, my name is John Riggi and I am the Senior Advisor for Cybersecurity and Risk at the American Hospital Association (AHA). On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 43,000 individual members, I thank you for the opportunity to testify on the important issue of the cybersecurity threats facing hospitals, health systems and the health care field. Today, I will discuss the nature of threats faced by hospitals and health systems, the unique challenges confronting the health care sector, and what the federal government can do to help ensure appropriate protections.

Hospitals, and health care overall, remain heavily targeted by cyber adversaries. The health care field is increasingly realizing the promise of networked information technologies to improve quality and patient safety and bring efficiencies to our systems. But with those opportunities come vulnerabilities to theft and threats to the security of personal information for patients and employees, billing records – even the function of medical devices. Increasingly, bad actors are using phishing emails, malware, and other tactics to attempt to attack hospital computers, networks, and connected devices.

Recently publicized attacks included the use of ransomware – software that holds computers hostage through malicious usage of encryption until a ransom is paid. Other attacks may be motivated by a desire to steal data from a health care system, such as individual medical, financial, or other identity information that can be monetized. In some cases, health care organizations may have intellectual property that is of interest to others. Recognizing that much of the data held by health care organizations is highly sensitive, as well as valuable, hospital and health system leaders are taking cybersecurity challenges extremely seriously and understand that protecting patients and their personal data is a 24/7 responsibility.

UNIQUE CHALLENGES FOR THE HEALTH CARE SECTOR

Health care providers are uniquely and heavily targeted due to the multiple valuable data sets they possess. For instance, recently published data[1] from the Ponemon Institute found the average cost for a lost or stolen health care record was $408 per record. However, the average cost for a lost or stolen record for all industries was much less, coming in at $148 per record. The average cost of a breach for all industries was $3.68 million dollars, while the average cost of a breach for a health care organization was approximately 2.75 times the industry average, or $10.6 million dollars.

Health care is the only economic sector that possesses highly targeted data sets such as personally identifiable information, payment information, protected health information, business intelligence, intellectual property related to medical research and innovation (including genomic studies related to the development of precision medicine), and, as a critical infrastructure sector, national security information related to emergency preparedness and response in times of national crisis or war.

Each one of these data sets are heavily targeted by cyber adversaries. Hospitals and health systems are the only organizations that may possess all of these data sets in combination. Individually, these data sets are highly valuable to the cyber adversary; in combination, they become exponentially valuable.

Also, health care records continue to command a premium price on the dark web because they have enduring value to the cyber adversary. In other words, unlike credit card numbers, one cannot cancel their blood type or a medical diagnosis. Stolen health care records may be the source of repeated health care fraud or be exploited on an ongoing basis for intelligence purposes by a nation-state.

THREATS TO HOSPITALS AND HEALTH SYSTEMS

The main cyber threats faced by hospitals and health care systems are external. They include:

- computer intrusions by external adversaries;
- crypto hijacking;
- business email compromise;
- ransomware attacks;

[1] Cost of Data Breach Study conducted by the Ponemon Institute https://www.ibm.com/security/data-breach

- supply chain attacks;
- data extortion; and
- denial-of-service attacks.

Of these, the most significant and common threats faced by our members include external computer intrusions, which cause the greatest loss of data and bear the highest associated costs in terms of remediation and lost revenue.

A new and emerging threat in 2018 relates to "crypto hijacking" refers to cybercriminals who penetrate a network and take over an organization's high-power computing resources for the purposes of cryptocurrency mining. The unauthorized malware and draining of computer resource may have serious consequences, including the potential disruption of hospital clinical and business operations, along with significant financial costs associated with remediation

Phishing emails continue to be one of the main attack vectors used by cyber adversaries to deliver malware into hospital and health system networks. As a result, hospitals screen incoming email very carefully. It is not uncommon for hospital network defenders to initially block 95 percent or more of incoming email traffic as potentially malicious or spam, accounting for millions of rejected emails every day.

Ransomware also continues to be a major threat for hospitals and health systems. Not only does ransomware hold data captive, it can potentially disrupt clinical and business operations, potentially interfering with the delivery of care and possibly impacting patient safety. More than 200,000 computers in more than 150 countries last year were infected with the WannaCry ransomware worm, which locked down systems and demanded a ransom payment to have them restored. While this attack was waged against all sectors, the health sector drew attention from the media and federal officials because of the critical nature of health care and the widespread impact of the attack on England's National Health Service. The impact on American hospitals and health systems was far less serious, which speaks to the tremendous efforts the field has made to improve cybersecurity and build incident response capabilities.

A WIDE RANGE OF CYBER ADVERSARIES

The U.S. government has attributed last year's WannaCry attack to North Korea. The vast majority of cyber adversaries are based overseas in generally non-cooperative jurisdictions. This general category of cyber adversaries is typically politically or ideologically motivated, such as Hacktivists and terrorists. Thankfully, there have been a very limited number of Hacktivist incidents targeting U.S. hospitals and no known incidences of foreign terrorist organizations conducting attacks against U.S. hospitals and health systems.

Other cyber adversaries include those who are criminally motivated and seek to steal data for illicit financial gain, such as foreign-based cyber organized crime groups. Under this category, health care also faces significant challenges from the criminally motivated insider who steals health records for financial gain and sometimes conspires with an external adversary to enable a cyber attack.

Finally, nation-states posing the most significant threats to hospitals and health systems include China, Russia, Iran, and North Korea. These nation-states, which sometimes operate in cooperation and collusion with criminal organizations, may have unique hacking capabilities. They may target hospitals and health systems to steal data to meet their intelligence requirements, or because of their national security or economic interests. The targeted data may include health records of individuals of intelligence interest, such as government and military personnel, politicians, private individuals possessing security clearances or with access to sensitive information, and individuals of influence.

HIPAA SECURITY RULE PROVIDES COMPREHENSIVE STANDARDS FOR HOSPITALS AND HEALTH SYSTEMS

From a regulatory point of view, health care entities already have significant obligations under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. That rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has responsibility for enforcing the Security Rule, with civil monetary penalties for violations. OCR has exercised this power in the past and remains a very active regulator. Failure to comply with HIPAA also can result in criminal penalties, and OCR may refer a complaint to the Department of Justice for investigation.

VICTIMS OF CYBER ATTACKS SHOULD BE GIVEN ASSISTANCE, NOT BLAME

Despite complying with rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated attacks, some of which will inevitably succeed. The government often repeats the phrase "It's not a matter of if, but when" in regard to an organization becoming a victim of a cyber attack. In fact, as the leader of the Federal Bureau of Investigation's (FBI) cyber national outreach section, I promoted the philosophy that organizations that were victims of breaches should be treated as victims of crime. This approach was subsequently codified in PPD-41.

The victims of attacks should be given support and resources, and attackers should be investigated and prosecuted. Merely because an organization was the victim of a cyber attack does not mean that the organization itself was in any way at fault or unprepared. Similarly, a breach does not necessarily equate to a HIPAA Security Rule compliance failure. In fact, an aggressive regulatory approach could be counter-productive and hinder valued cooperation by the victims of cyber attack with other parts of the government, such as the Department of Homeland Security (DHS), FBI and the intelligence community. Instead, successful attacks should be fully investigated, and the lessons learned should be widely disseminated to prevent the success of similar attacks in the future.

COORDINATED GOVERNMENT SUPPORT AND PARTNERSHIP ARE KEY TO STOPPING CYBER CRIME

Despite hospitals' concerted attempts to secure their cyber ecosystems, individual efforts to secure systems are insufficient to prevent all attacks. The Administration has used executive orders to name 16 critical infrastructure sectors — including health care and public health —

deemed essential to the security of the nation and directed federal agencies to prioritize securing federal systems. HHS is designated as the liaison for the health care sector. More broadly, the FBI has been designated as the lead authority on investigating cybercrime. Other agencies, including the DHS and the Secret Service, also play key roles in combatting cybercrime and providing guidance. Coordination across these federal resources is critical to ensure threat intelligence and defensive strategies are shared widely, effectively, and in a timely manner. In addition, these agencies must be given the resources to not only respond to attacks, but help vulnerable health care targets prevent attacks from occurring or succeeding on an ongoing basis.

The Cybersecurity Information Sharing Act of 2015 (CISA) provided a mechanism for information sharing among private-sector and federal government entities and provides a safe harbor from certain liabilities related to that information sharing. Information sharing allows organizations to stay ahead of emerging cybersecurity risks and contribute to collective knowledge of threats to guard against. Several private-sector entities, such as the Nation's Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC) and Health Information Trust Alliance (HITRUST), provide information-sharing opportunities. In addition, the federal government has provided information-sharing resources through its cybersecurity initiatives, including health care and public health facilities. With that said, the goals of information sharing have yet to be fully realized. Expedited and tailored cyber threat information sharing from the federal government would benefit all health care and public health organizations. Providers most need actionable information that identifies specific steps they can take to secure against new threats. Large volumes of more generalized information can prove challenging to interpret, and even become a distraction.

HHS also is directed under CISA to work with the private sector and other federal agencies to establish voluntary, consensus-based best practices. While the federal government is working to provide additional educational and other resources to the health care field overall, more action is needed to address the cybersecurity challenges facing all sectors, including health care. As a nation, we must bolster the security of our cyber ecosystem, not just place the burden on individual institutions. Indeed, the magnitude of the challenges and the growing sophistication of the attacks suggests that the federal government must provide additional nationwide resources. These include efforts to:

- Develop and disseminate coordinated national defensive measures;
- Strengthen and expand our cybersecurity workforce through grant programs and retraining efforts, perhaps with a particular focus on the retraining of veterans;
- Identify and disrupt bad actors;
- Increase the consequences for those who commit cybercrimes; and
- Identify and support best practices by the private sector.

CONCLUSION

Hospitals and health systems are heavily targeted by cyber adversaries, which include sophisticated nation-states. Hospitals and health systems have made great strides to defend their networks, secure patient data, preserve the efficient delivery of health care services and, most

importantly, protect patient safety. However, we cannot do it alone – we need more active support from the government to defend patients from cyber threats. Conversely, the government cannot protect our nation from cyber criminals alone either – they need the expertise and exchange of cyber threat information from the field to effectively combat cyber threats. What is truly needed is the government and health care sector working in close cooperation with a formal exchange of cyber threat information – truly a "Whole of Nation Approach."

Mr. PALMER. I thank the gentleman.

The chair now recognizes Mr. Weissman for his testimony.

STATEMENT OF ROBERT WEISSMAN

Mr. WEISSMAN. Mr. Palmer and Mr. Raskin, thank you very much for the opportunity to speak today. I wanted to make three general points and, assuming I talk fast enough, add a footnote in.

The American regulatory system has made our country stronger, better, safer, cleaner, healthier, more fair, and more just. It's something we should be celebrating, trying to improve, but not attacking with evidence-free allegations.

As Mr. Raskin pointed out, the benefits of regulation, Federal regulation, even monetized and corporate-friendly accounting systems, vastly exceed the costs. We know that because of the OMB reviews of the costs and benefits of significant regulations issued each year. Every single year since the agency started conducting that study in 2001, benefits have vastly exceeded costs at minimum of a range of 2 to 1 and typically up to 12 to 1.

Critics of regulation too often focus on costs to the exclusion of talking about the benefits. No agency adopts a rule for the simple purpose of imposing costs. There's always a rationale and reason, and the benefits have to be taken into account. The $2 trillion figure that is routinely cited is not based on careful analysis, as my testimony describes in some detail.

It's worth focusing also for a moment on the American Hospital Association study, which fell into this same problem of focusing exclusively on the cost of regulation without talking about the benefit. It acknowledges that there may be some patient benefits, but doesn't actually try to monetize those costs.

The study does not show that there are duplicative regulations. The study does not acknowledge the benefits in monetary terms to patients. The study does not disclose its methodology or how its survey was calculated. So there's every reason to assume that the cost estimates are inflated.

Most importantly, what the study fails to do is acknowledge why it is that the government imposes a host of regulations on the healthcare sector. It's primarily to deal with two overarching problems: poor quality of care and massive fraud.

250,000 people die every single year in this country from medical malpractice, making it the third highest single cause of death in this country. By any metric, we perform at often the worst of all rich countries in quality of care.

Quality of care regulations are aimed at trying to improve that situation. Fraud consumes 3 to 10 percent of all healthcare spending in the United States, according to the FBI. At the low end, $80 billion a year.

Those regulations are designed to cut down on rampant fraud. They have a purpose. They are inadequate. They're obviously not doing the job. It would be much worse off if those rules, by and large, were not in place.

The second point I wanted to make was about the issue of regulatory duplication. I think it is the case that much of what's complained about in the area of duplication is really a disguised complaint about regulation itself.

That said, there are obviously, in a complicated bureaucracy, in a complicated economy, overlapping rules and regulations and massive regulatory gaps. So for sure better coordination is desirable. It doesn't really make sense to blame that problem on the administrative state, though.

Let's talk for a moment about cybersecurity. It is the case that there are massive gaps in cybersecurity and privacy protections in this country. That's because there is no overarching American cybersecurity framework or privacy protection law.

We absolutely need that. I detail some components of what would be desirable in such a framework. That may not cure all the problems that are being discussed today by area specialists, but it would for sure deal with many of them.

The third thing I wanted to highlight is that, although there has been a very partisan discussion about regulation in the Congress for now going on almost a decade, there is a shared agenda that's available if members are eager to pick it up.

I think the key elements of reform packages that would have bipartisan support would focus on transparency, limiting regulatory delay, enhancing regulatory enforcement without regard to adopting new rules but making sure everyone plays by the same rules, and focusing on the revolving door of people leaving from regulatory agencies and going into regulated industry, and back and forth.

Finally, my footnote. Yesterday my organization, along with 100 other organizations, petitioned OSHA to adopt a heat standard to protect indoor and outdoor workers from extreme heat. More than 1,000 people die every near in this country from extreme heat. Many of them are workers, especially agricultural workers.

Supporting our petition was Raudel Felix Garcia, the brother of Audon Felix Garcia, a California farmworker who died from excessive heat in the fields. Raudel told the story of his brother's death yesterday in a teleconference we had in wrenching detail and pleaded with Federal regulators to take steps to make sure that no one else died such a needless death.

It was a crucial reminder both in that particular area, but more generally, that life and death is at stake in regulation, that real people are affected and protected and need strong regulatory protections. And I hope this Congress can ensure that that is delivered to them.

Thank you very much.

[Prepared statement of Mr. Weissman follows:]

Written Testimony of

Robert Weissman
President, Public Citizen

before the

The House Oversight Committee
Subcommittee on Intergovernmental Affairs

on

"Regulatory Divergence:
Failure of the Administrative State"

July 18, 2018

Mr. Chairman and Members of the Committee,

Thank you for the opportunity to testify today on regulatory policy issues. I am Robert Weissman, president of Public Citizen. Public Citizen is a national public interest organization with more than 400,000 members and supporters. For more than 45 years, we have advocated with some considerable success for stronger health, safety, consumer protection and other rules, as well as for a robust regulatory system that curtails corporate wrongdoing and advances the public interest.

Public Citizen chairs the Coalition for Sensible Safeguards (CSS). CSS is an alliance of more than 100 consumer, small business, labor, scientific, research, good government, faith, community, health and environmental organizations joined in the belief that our country's system of regulatory safeguards provides a stable framework that secures our quality of life and paves the way for a sound economy that benefits us all. My testimony today, however, is solely on behalf of Public Citizen.

Over the last century, and up to the present, regulations have made our country stronger, better, safer, cleaner, healthier and more fair and just. Regulation is one of the greatest public policy success stories in terms of benefits to the public and is a testament to the power of Congress in protecting the public through passage of critical, foundational laws such as the Clean Air Act, the Clean Water Act, the Occupational Safety and Health Act, the Consumer Product Safety Act, the Civil Rights Act, various food safety laws, and many more. Strong and effective public health and safety regulations are a reflection of Congress' desire to protect everyday Americans through laws that are still among the most popular and cherished by the public.

Unfortunately, this Administration has sought to roll back regulatory safeguards in radical and unprecedented fashion. Two recent Public Citizen reports, "Sacrificing Public Protections on the Altar of Deregulation" and "Deregulatory Frenzy," based on detailed empirical analysis of data disclosed in the first three Unified Regulatory Agendas of the Trump administration, present a full accounting of hundreds of regulatory protections that were unilaterally withdrawn by agencies under the Trump Administration.[1] In addition, Congress has resorted to the Congressional Review Act, which bypasses normal legislative procedures, in order to repeal more than a dozen critical regulatory protections[2] that were issued near the end of the previous administration, plus a crucial consumer protection measure from the Consumer Financial Protection Bureau. Finally, agencies have begun the process of repealing rules finalized under the last administration and delaying others indefinitely by categorizing them as "long term" actions in the most recent Unified Regulatory Agenda.[3]

---

[1] Michael Tanglis, *Sacrificing Public Protections on the Altar of Deregulation*, Public Citizen, November 28, 2017. Available at: https://www.citizen.org/sites/default/files/trump-withdrawn-regs-report.pdf; and Michael Tanglis, *Deregulatory Frenzy*, Public Citizen, June 5, 2018. Available at: https://www.citizen.org/sites/default/files/deregulatory_frenzy_final.pdf

[2] Coalition for Sensible Safeguards, Rules at Risk, Public Citizen, 2018. Available at: https://rulesatrisk.org/

[3] Spring 2018 Unified Agenda of Regulatory and Deregulatory Actions, Office of Information and Regulatory Affairs. Available at: https://www.reginfo.gov/public/do/eAgendaMain

President Trump's Executive Order on regulations, 13771,[4] is a key driver of deregulatory activity at all agencies. EO 13771 restricts an agency from issuing the most important and beneficial new regulations (i.e. significant regulations) unless the agency is first able to identify and remove at least two existing regulations and unless repealing those existing regulations results in costs savings that fully offset costs imposed by the new regulation. In other words, agencies are only allowed to protect the public to the extent that it imposes no new costs on corporations. Further, the EO places pressure on each agency to ensure that any regulatory protections the agency seeks to adopt must be fashioned in a way that minimizes costs in order to comply with regulatory budgets imposed under the EO, rather than in a way that maximizes the effectiveness and benefits of the regulatory protection to the public. Agencies have identified hundreds of crucial public protections that are subject to EO 13771[5] and, thus, that cannot be issued unless offset by deregulatory actions. Among those protections are new lead in drinking water standards, new gun control measures, new car, truck, and train safety standards, new environmental protections including restrictions on toxic chemicals, safety standards for tobacco products like e-cigarettes, numerous workplace safety protections, and updates to energy efficiency standards.

President Trump has justified his deregulatory agenda as a means to create economic growth. After one year, the evidence is clear that deregulation is causing no such economic growth. Both GDP and jobs figures show that there has been no greater economic growth under this administration than the last.[6] A January 2017 report by Goldman Sachs studied whether job growth and capital spending have been stronger in sectors and companies that were more highly regulated before the most recent election. According to the report, "[W]e find no evidence that employment or capital spending accelerated more after the election in areas where regulatory burdens are higher." Overall, Goldman found, "Our results suggest that non-financial deregulation has had a limited impact on the economy to date." These results are "not that surprising," including because "the estimated costs of regulation are not that high."[7]

By contrast, as we have seen in recent years, the cost of regulatory failure — lack of regulatory enforcement, regulations delayed or rolled back, and insufficient regulatory standards and protections in place — is often immense, whether measured in lives lost, injuries incurred, environmental damage inflicted, families and communities disrupted and national economic loss. Most notably, regulatory failure was significantly responsible for the Great Recession, which imposed far greater costs on the economy and cost far more jobs than regulations ever could.

The first section of this testimony provides a quick overview of how regulations strengthen

---

[4] Executive Order 13771, January 30, 2017. Available at: https://www.federalregister.gov/documents/2017/02/03/2017-02451/reducing-regulation-and-controlling-regulatory-costs

[5] In the most recent Unified Regulatory Agenda of Fall 2017, agencies have begun identifying regulatory actions listed on the Agenda as "regulatory," "deregulatory"]," or otherwise "exempt" for purposes of EO 13771.

[6] Jennifer Rubin, President Trump's Deregulation Flop, The Washington Post, February 13, 2018. Available at: https://www.washingtonpost.com/blogs/right-turn/wp/2018/02/13/president-trumps-deregulation-flop/?utm_term=.a97ce3cff3ae

[7] James Pethokoukis, What's been the economic impact of Trump's deregulation push? American Enterprise Institute, February 12, 2018. Available at: http://www.aei.org/publication/whats-been-the-economic-impact-of-trumps-deregulation-push/

America. The second section explains that regulations are economically smart, by examining relevant aggregate data. It also debunks empirically starved and groundless claims about enormous regulatory cost, and recounts the history of regulated industry's Chicken Little claims about the devastating impact of proposed rules. The third section offers case studies to show that regulations are economically smart. It reviews how regulatory failure led to the Great Recession with its horrific human and economic toll; examines ongoing problems in the financial sector through the examples of Wells Fargo and Equifax; explains how the Clean Car rule now facing roll back would both protect the planet and save consumers hundreds of billions of dollars; and reports on the detrimental impact of the administration's effort to block and replace the Department of Education's Borrower Defense rule. The fourth section looks at sectoral issues related to purported regulatory duplication, in the areas of cybersecurity, financial regulation and health care regulation. The final section briefly concludes with a call for a new turn in the regulatory policy debate.

I. Regulations Strengthen America

This hearing is unfortunately framed around the purported "failure of the administrative state." It makes little sense to consider costs of regulation, however, without recognizing regulatory benefits.

Our country has made dramatic gains through regulation, making the country safer, healthier, more just, cleaner, more equitable and more financially secure. Regulation has made all of our lives better. It has:

- Made our food safer.[8]
- Saved tens of thousands of lives by making our cars safer. NHTSA's vehicle safety standards have reduced the traffic fatality rate from nearly 3.5 fatalities per 100 million vehicles traveled in 1980 to 1.41 fatalities per 100 million vehicles traveled in 2006. [9]
- Made it safer to breathe, saving hundreds of thousands of lives annually. Clean Air Act rules saved 164,300 adult lives in 2010. In February 2011, EPA estimated that by 2020 they will save 237,000 lives annually. EPA air pollution controls saved 13 million days of lost work and 3.2 million days of lost school in 2010, and EPA estimates that they will save 17 million work-loss days and 5.4 million school-loss days annually by 2020. [10]
- Protected children's brain development by phasing out leaded gasoline. EPA regulations phasing out lead in gasoline helped reduce the average blood lead level in U.S. children ages 1 to 5. During the years 1976 to 1980, 88 percent of all U.S. children had blood

[8] In addition to the historic advances through food safety regulation, implementation of the 2011 Food Safety Modernization Act will have tremendous benefits, eliminating most of the annual toll of 48 million illnesses, 128,000 hospitalizations, and 3,000 deaths that the Centers for Disease Control and Prevention estimates occur each year from contaminated food. Taylor, M. (February 5, 2014). *Implementing the FDA Food Safety Modernization Act*, available at: http://www.fda.gov/NewsEvents/Testimony/ucm384687.htm.

[9] Steinzor, R., & Shapiro, S. (2010). *The People's Agents and the Battle to Protect the American Public: Special Interests, Government, and Threats to Health, Safety, and the Environment*: University of Chicago Press.

[10] *See* U.S. Environmental Protection Agency, Office of Air and Radiation. (2011, March). *The Benefits and Costs of the Clean Air and Radiation Act from 1990 to 2020*. Available at: http://www.epa.gov/oar/sect812/feb11/fullreport.pdf..

levels in excess of 10 micrograms/deciliter; during the years 1991 to 1994, only 4.4 percent of all U.S. children had blood levels in excess of that dangerous amount. [11]

- Empowered disabled persons by giving them improved access to public facilities and workplace opportunities, through implementation of the Americans with Disabilities Act.[12]
- Guaranteed a minimum wage, ended child labor and established limits on the length of the work week.[13]
- Saved the lives of thousands of workers every year. Deaths on the job have declined from more than 14,000 per year in 1970, when the Occupational Safety and Health Administration was created, to under 4,500 at present. [14]
- Protected the elderly and vulnerable consumers from a wide array of unfair and deceptive advertising techniques.[15]
- For half a century in the mid-twentieth century, and until the onset of financial deregulation, provided financial stability and a right-sized financial sector, helping create the conditions for robust economic growth and shared prosperity.[16]

These are not just the achievements of a bygone era. Regulation continues to improve the quality of life for every American, every day. Ongoing and emerging problems and a rapidly changing economy require the issuance of new rules to ensure that America is strong and safe, healthy and wealthy.

II. Regulations are Economically Smart: Aggregate Data

Although most regulations do not have economic objectives as their primary purpose, in fact regulation is overwhelmingly positive for the economy.

While regulators commonly do not have economic growth and job creation as a mission priority, they are mindful of regulatory cost, and by statutory directive or on their own initiative typically

---

[11] Office of Management and Budget, Office of Information and Regulatory Affairs. (2011). *2011 Report to Congress on the Benefits and Costs of Federal Regulations an Unfunded Mandates on State, Local, and Tribal Entities*. Available at: http://www.whitehouse.gov/sites/default/files/omb/inforeg/2011_cb/2011_cba_report.pdf.

[12] National Council on Disability. (2007). *The Impact of the Americans with Disabilities Act*. Available at: http://www.ncd.gov/publications/2007/07262007.

[13] There are important exceptions to the child labor prohibition; significant enforcement failures regarding the minimum wage, child labor and length of work week (before time and a half compensation is mandated). But the quality of improvement in American lives has nonetheless been dramatic. Lardner, J. (2011). *Good Rules: 10 Stories of Successful Regulation*. Demos. Available at: http://www.demos.org/sites/default/files/publications/goodrules_1_11.pdf.

[14] *See* AFL-CIO. (2015, April.) *Death on the Job: The Toll of Neglect*. p. 1. Available at: http://www.aflcio.org/content/download/154671/3868441/DOTJ2015Finalnobug.pdf. Mining deaths fell by half shortly after creation of the Mine Safety and Health Administration. Weeks, J. L., & Fox, M. (1983). Fatality rates and regulatory policies in bituminous coal mining, United States, 1959-1981. *American journal of public health, 73*(11), 1278.

[15] See 16 CFR 410-460.

[16] See Stiglitz, J. E. (2010). *Freefall: America, free markets, and the sinking of the world economy*: WW Norton & Co Inc.; Kuttner, R. (2008). *The Squandering of America: how the failure of our politics undermines our prosperity*: Vintage.

seek to minimize costs; relatedly, the rulemaking process gives affected industries ample opportunity to communicate with regulators over cost concerns, and these concerns are taken into account. To review the regulations actually proposed and adopted is to see how much attention regulators pay to reducing cost and detrimental impact on employment. And to assess the very extended rulemaking process is to see how substantial industry influence is over the rules ultimately adopted — or discarded.

In trying to get a handle on actual costs and benefits of regulation, much more informative than theoretical work, anecdotes and allegations is a review of the actual costs and benefits of regulations — though even this methodology is significantly imprecise and heavily biased against the benefits of regulation. Every year, the Office of Management and Budget analyzes the costs and benefits of rules with significant economic impact. While the Trump administration released the most recent report well past the deadline imposed by Congress and with little publicity, it one again showed that the benefits massively exceed costs.

The principle finding of *OMB's draft 2017 Report to Congress on the Benefits and Costs of Federal Regulation* is:

> The estimated annual benefits of major Federal regulations reviewed by OMB from October 1, 2006, to September 30, 2016, for which agencies estimated and monetized both benefits and costs, are in the aggregate between $219 billion and $695 billion, while the estimated annual costs are in the aggregate between $59 billion and $88 billion, reported in 2001 dollars. In 2015 dollars, aggregate annual benefits are estimated to be between $287 and $911 billion and costs between $78 and $115 billion. These ranges reflect uncertainty in the benefits and costs of each rule at the time that it was evaluated.[17]

In other words, even by OMB's most conservative accounting, the benefits of major regulations over the last decade exceeded costs by a factor of more than two-to-one. And benefits may exceed costs by a factor of 12.

These results are consistent year-to-year as the following table shows.

[17] Office of Management and Budget, Office of Information and Regulatory Affairs. (2015). Draft *2015 Report to Congress on the Benefits and Costs of Federal Regulations an Unfunded Mandates on State, Local, and Tribal Entities. pp.1-2.* Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/draft_2017_cost_benefit_report.pdf.

Total Annual Benefits and Costs of Major Rules by Fiscal Year (billions of 2001 dollars)[18]

Fiscal Year	Number of Rules	Benefits	Costs
2001	12	22.5 to 27.8	9.9
2002	2	1.5 to 6.4	0.6 to 2.2
2003	6	1.6 to 4.5	1.9 to 2.0
2004	10	8.8 to 69.8	3.0 to 3.2
2005	12	27.9 to 178.1	4.3 to 6.2
2006	7	2.5 to 5.0	1.1 to 1.4
2007	12	28.6 to 184.2	9.4 to 10.7
2008	11	8.6 to 39.4	7.9 to 9.2
2009	15	8.6 to 28.9	3.7 to 9.5
2010	18	18.6 to 85.9	6.4 to 12.4
2011	13	34.3 to 98.5	5.0 to 10.2
2012	14	53.2 to 114.6	14.8 to 19.5
2013	7	25.6 to 67.3	2.0 to 2.5
2014	13	8.1 to 18.9	2.5 to 3.7
2015	21	19.6 to 36.9	4.2 to 5.3
2016	16	13.6 to 27.3	3.3 to 4.9

The reason for the consistency is that regulators pay a great deal of concern to comparative costs and benefits (even though there is, we believe, a built-in bias of formal cost-benefit analysis against regulatory initiative[19]). Very few major rules are adopted where projected costs exceed projected benefits, and those very few cases typically involve direct Congressional mandates.

It should also be noted that relatively high regulatory compliance costs do not necessarily have negative job impacts; firm expenditures on regulatory compliance typically create new jobs within affected firms or other service or product companies with which they contract.

Moreover, the empirical evidence also fails to support claims that regulation causes significant job loss. Insufficient demand is the primary reason for layoffs. In extensive survey data collected by the Bureau of Labor Statistics, employers cited lack of demand roughly 100 times more

---

[18] Office of Management and Budget, Office of Information and Regulatory Affairs. (2017). *Draft 2017 Report to Congress on the Benefits and Costs of Federal Regulations an Unfunded Mandates on State, Local, and Tribal Entities. Table 1-4,* pp. 19-20. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/draft_2017_cost_benefit_report.pdf; 2001-2006 data from: Office of Management and Budget, Office of Information and Regulatory Affairs. (2011). *2011 Report to Congress on the Benefits and Costs of Federal Regulations an Unfunded Mandates on State, Local, and Tribal Entities. Table 1-3,* p. 19-20. Available at: http://www.whitehouse.gov/sites/default/files/omb/inforeg/2011_cb/2011_cba_report.pdf.

[19] *See, e.g.*, Shapiro, S. et al., *CPR Comments on Draft 2010 Report to Congress on the Benefits and Costs of Federal Regulations* 16-19 (App. A, Pt. C.) (2010), Available at: http://www.progressivereform.org/articles/2010_CPR_Comments_OMB_Report.pdf ; Steinzor, R. et al., *CPR Comments on Draft 2009 Report to Congress on the Benefits and Costs of Federal Regulations* 16-19 (App. A, Pt. C.) (2009), Available at: http://www.progressivereform.org/articles/2009_CPR_Comments_OMB_Report.pdf.

frequently than government regulation as the reason for mass layoffs![20] (Unfortunately, in response to budget cuts, the BLS ceased producing its mass layoff report in 2013.)

Reason for layoff: 2008-2012[21]

	2008	2009	2010	2011	2012
Business Demand	516,919	824,834	384,564	366,629	461,328
Governmental regulations/intervention	5,505	4,854	2,971	2,736	3,300

It is also the case that firms typically innovate creatively and quickly to meet new regulatory requirements, even when they fought hard against adoption of the rules.[22] The result is that costs are commonly lower than anticipated.

There is, to be sure, a large body of theoretical and non-empirical work on the cost of regulation, some of which yields utterly implausible cost estimates. Most prominent in this regard is the report issued by Nicole Crain and W. Mark Crain, consultants to the Small Business Administration Office of Advocacy.[23] This study is thoroughly discredited, but the study's groundless conclusions (that regulation costs the U.S. economy $1.75 trillion annually, or more than $10,000 per small business employee) continues to be cited too frequently in policy debates, often without attribution to the original, discredited study. Crain and Crain attribute $1.236 trillion in costs to "economic regulation." This concept as employed by Crain and Crain includes a range of elements that might properly be considered regulation, but which are not typically part of the regulatory policy debate. This includes matters such as tariffs, antitrust policy, complexity of the tax system, and ease of starting a new business,[24] a figure that is entirely derived from a regression analysis correlating ratings on a World Bank "regulatory quality index" — which is itself based on nothing more than survey data from businesses and other sources — and national GDP per capita. It is remarkable enough to imagine that such a cross-cultural, international regression analysis would yield such a robust result that it should meaningfully inform U.S.

---

[20] U.S. Department of Labor, Bureau of Labor Statistics. (2012, November). *Extended Mass Layoffs in 2011. Table 5. Reason for layoff: extended mass layoff events, separations, and initial claimants for unemployment insurance, private nonfarm sector, 2009-2011.* Available at: http://www.bls.gov/mls/mlsreport1039.pdf.

[21] U.S. Department of Labor, Bureau of Labor Statistics. (2012, November). *Extended Mass Layoffs in 2011. Table 5. Reason for layoff: extended mass layoff events, separations, and initial claimants for unemployment insurance, private nonfarm sector, 2010-2012.* Available at: http://www.bls.gov/mls/mlsreport1043.pdf. U.S. Department of Labor, Bureau of Labor Statistics. (2013, September). *Extended Mass Layoffs in 2011. Table 4. Reason for layoff: extended mass layoff events, separations, and initial claimants for unemployment insurance, private nonfarm sector, 2009-2011.* Available at: http://www.bls.gov/mls/mlsreport1039.pdf ; U.S. Department of Labor, Bureau of Labor Statistics. (2011, November). *Extended Mass Layoffs in 2010. Table 6. Reason for layoff: extended mass layoff events, separations, and initial claimants for unemployment insurance, private nonfarm sector, 2008-2010.* Available at: http://www.bls.gov/mls/mlsreport1038.pdf.

[22] Mouzoon, N., & Lincoln, T. (2011). *Regulation: The Unsung Hero in American Innovation.* Public Citizen. Available at: http://www.citizen.org/documents/regulation-innovation.pdf.

[23] Crain, N. V., & Crain, W. M. (2010). *The Impact of Regulatory Costs on Small Firms. Prepared for Small Business Administration*, Office of Advocacy. Available at: http://archive.sba.gov/advo/research/rs371tot.pdf.

[24] Crain, N. V., & Crain, W. M. (2010). *The Impact of Regulatory Costs on Small Firms. Prepared for Small Business Administration*, Office of Advocacy. Available at: http://archive.sba.gov/advo/research/rs371tot.pdf.

policy; even more so, when it yields a total cost vastly out of line with other careful analysis, as well as such unlikely findings as a correlation between increased education and reduced economic growth. It turns out, as the Economic Policy Institute has shown, that with a more complete set of data than used by Crain and Crain — but still using the same regression equations — no statistical relationship between "regulatory quality" and GDP exists.[25] Crain and Crain also include a cost for tax compliance — not typically considered a "regulatory" cost — which they pin at roughly $160 billion. A number of other fatal flaws bedevil the discredited study.[26] The Crain and Crain study is characteristic of other poorly constructed anti-regulatory studies, which purport to tally costs of regulation but ignore benefits.

There is also a long history of business complaining about the cost of regulation — and predicting that the next regulation will impose unbearable burdens:

- Bankers and business leaders described the New Deal financial regulatory reforms in foreboding language, warning that the Federal Deposit Insurance Commission and related agencies constituted "monstrous systems," that registration of publicly traded securities constituted an "impossible degree of regulation," and that the New Deal reforms would "cripple" the economy and set the country on a course toward socialism.[27] In fact, those New Deal reforms prevented a major financial crisis for more than half a century — until they were progressively scaled back.
- Chemical industry leaders said that rules requiring removal of lead from gasoline would "threaten the jobs of 14 million Americans directly dependent and the 29 million Americans indirectly dependent on the petrochemical industry for employment." In fact, while banning lead from gasoline is one of the single greatest public policy public health accomplishments, the petrochemical industry has continued to thrive. The World Bank finds that removing lead from gasoline has a ten times economic payback.[28]
- Big Tobacco long convinced restaurants, bars and small business owners that smokefree rules would dramatically diminish their revenue — by as much as 30 percent, according to industry-sponsored surveys. The genuine opposition from small business owners — based on the manipulations of Big Tobacco — delayed the implementation of smokefree rules and cost countless lives. Eventually, the Big Tobacco-generated opposition was overcome, and smokefree rules have spread throughout the country — significantly lowering tobacco consumption. Dozens of studies have found that smokefree rules have had a positive or neutral economic impact on restaurants, bars and small business.[29]

---

[25] Irons, J., & Green, A. (2011, 19 July). *Flaws Call For Rejecting Crain and Crain Model*. Economic Policy Institute. Retrieved 24 February, 2012, from http://www.epi.org/page/-/EPI_IssueBrief308.pdf.

[26] Eisenbrey, R., & Shapiro, I. (2011, August). *Deconstructing Crain and Crain*. Economic Policy Institute. Retrieved 24 February, 2012, from http://web.epi-data.org/temp727/IssueBrief312-2.pdf.; Irons, J. and Green, A., *Flaws Call for Rejecting Crain and Crain Model*.; Shapiro, S. A., & Ruttenberg, R. (2011, February). *The Crain and Crain Report on Regulatory Costs*. Center for Progressive Reform. Retrieved 24 February, 2012, from http://www.progressivereform.org/articles/SBA_Regulatory_Costs_Analysis_1103.pdf; Copeland, C. W. (2011, April 6). *Analysis of an Estimate of the Total Costs of Federal Regulations*. Congressional Research Service. Retrieved 24 February, 2012, from http://www.progressivereform.org/articles/CRS_Crain_and_Crain.pdf.

[27] Lincoln, T. (2011). *Industry Repeats Itself: The Financial Reform Fight*. Public Citizen. Available at: http://www.citizen.org/documents/Industry-Repeats-Itself.pdf.

[28] Crowther, A. (2013). *Regulation Issue: Industry's Complaints About New Rules Are Predictable — and Wrong. p.*8. Available at: http://www.citizen.org/documents/regulation-issue-industry-complaints-report.pdf.

[29] *Regulation Issue: Industry's Complaints About New Rules Are Predictable — and Wrong.* p.10.

- Rules to confront acid rain have reduced the stress on our rivers, streams and lakes, fish and forests.[30] Industry projected costs of complying with acid rain rules of $5.5 billion initially, rising to $7.1 billion in 2000; ex-ante estimates place costs at $1.1 billion - $1.8 billion.[31]
- In the case of the regulation of carcinogenic benzene emissions, "control costs were estimated at $350,000 per plant by the chemical industry, but soon thereafter the plants developed a new process in which more benign chemicals could be substituted for benzene, thereby reducing control costs to essentially zero."[32]
- The auto industry long resisted rules requiring the installation of air bags, publicly claiming that costs would be more than $1000-plus for each car. Internal cost estimates actually showed the projected cost would be $206.[33] The cost has now dropped significantly below that. The National Highway Traffic Safety Administration estimates that air bags saved 2,300 lives in 2010, and more than 30,000 lives from 1987 to 2010.[34]
- Similarly, the auto industry threatened doom if forced to adopt catalytic converter technology, saying that as a result of such a mandate, "the prospect of unreasonable risk of business catastrophe and massive difficulties with these vehicles in the hands of the public may be faced. It is conceivable that complete stoppage of the entire production could occur, with the obvious tremendous loss to the company, shareholders, employees, suppliers, and communities."[35]

There is a long list of other examples from the last century — including child labor prohibitions, the Family Medical Leave Act, the CFC phase out, asbestos rules, coke oven emissions, cotton dust controls, strip mining, vinyl chloride[36] — that teach us to be wary of Chicken Little warnings about the costs of the next regulation.

The important lessons here are that impacted industries have a natural bias to overestimate costs of regulatory compliance, and projections of cost regularly discount the impact of technological dynamism. Indeed, regulation spurs innovation and can help create efficiencies and industrial development wholly ancillary to its directly intended purpose.

---

[30] Environmental Protection Agency. *Acid Rain in New England: Trends.* Available at: http://www.epa.gov/region1/eco/acidrain/trends.html.

[31] The Pew Environment Group. (2010, October). *Industry Opposition to Government Regulation*. Available at: http://www.pewenvironment.org/uploadedFiles/PEG/Publications/Fact_Sheet/Industry%20Clean%20Energy%20Factsheet.pdf.

[32] Shapiro, I., & Irons, J. (2011). *Regulation, Employment, and the Economy: Fears of job loss are overblown*. Economic Policy Institute. Available at: http://www.epi.org/files/2011/BriefingPaper305.pdf.

[33] Behr, P. (August 13, 1981). U.S. Memo on Air Bags in Dispute. Washington Post.

[34] National Highway Traffic Safety Administration. (2012). *Traffic Safety Facts: Occupant Protection*. Available at: http://www-nrd.nhtsa.dot.gov/Pubs/811619.pdf.

[35] April 11, 1973, hearing transcript cited in Clarence Ditlow, Federal Regulation of Motor Vehicle Emissions under the Clean Air Act Amendments of 1970, Ecological Law Journal, 1975, pp. 495-504

[36] *Regulation Issue: Industry's Complaints About New Rules Are Predictable — and Wrong*; Hodges, H. (1997). Falling Prices: Cost of Complying With Environmental Regulations Almost Always Less Than Advertised. Economic Policy Institute. Available at: http://www.epi.org/publication/bp69 ; Shapiro, I., & Irons, J. (2011). *Regulation, Employment, and the Economy: Fears of job loss are overblown*. Economic Policy Institute. Available at: http://www.epi.org/files/2011/BriefingPaper305.pdf.

III. Regulations Are Economically Smart: Case Studies

A. Job-destroying regulatory failure and the Great Recession

Missing from much of the current policy debate on jobs and regulation is a crucial, overriding fact: The Great Recession and ongoing weakness in wage growth and the still-pervasive sense of economic insecurity are a direct result of too little regulation and too little regulatory enforcement. The costs of this set of regulatory failures are staggeringly high, and far outdistance any plausible story about the "cost" of regulation.

A very considerable literature, and a very extensive Congressional hearing record, documents in granular detail the ways in which regulatory failure led to financial crash and the onset of the Great Recession. "Widespread failures in financial regulation and supervision proved devastating to the stability of the nation's financial markets," concluded the Financial Crisis Inquiry Commission.[37] "Deregulation went beyond dismantling regulations," notes the Financial Crisis Inquiry Commission. "[I]ts supporters were also disinclined to adopt new regulations or challenge industry on the risks of innovations."[38]

The regulatory failures were pervasive, the Financial Crisis Inquiry Commission concluded:

> The sentries were not at their posts, in no small part due to the widely accepted faith in the self-correcting nature of the markets and the ability of financial institutions to effectively police themselves. More than 30 years of deregulation and reliance on self-regulation by financial institutions, championed by former Federal Reserve Chairman Alan Greenspan and others, supported by successive administrations and Congresses, and actively pushed by the powerful financial industry at every turn, had stripped away key safeguards, which could have helped avoid catastrophe. This approach had opened up gaps in oversight of critical areas with trillions of dollars at risk, such as the shadow banking system and over-the-counter derivatives markets. In addition, the government permitted financial firms to pick their preferred regulators in what became a race to the weakest supervisor.

A sampling of the very extensive regulatory failures that contributed to the crisis include:

> **Failure to stop toxic and predatory mortgage lending that blew up the housing bubble.** Concludes the Financial Crisis Inquiry Commission: "The prime example is the Federal Reserve's pivotal failure to stem the flow of toxic mortgages, which it could have done by setting prudent mortgage-lending standards. The Federal Reserve was the one entity empowered to do so and it did not."[39] Regulators failed almost completely to use then-existing authority to crack down on abusive lending practices. The Federal Reserve

---

[37] Financial Crisis Inquiry Commission. (2011). *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*. Washington, D.C.: Government Printing Office. p. 30.

[38] *The Financial Crisis Inquiry Report.* p. 53.

[39] *The Financial Crisis Inquiry Report.* p. xvii.

took three formal actions against subprime lenders from 2002 to 2007.[40] The Office of Comptroller of the Currency, with authority over almost 1,800 banks, took three consumer-protection enforcement actions from 2004 to 2006.[41]

Repeal of the Glass-Steagall Act. The Financial Services Modernization Act of 1999 formally repealed the Glass-Steagall Act of 1933 (also known as the Banking Act of 1933) and related laws, which prohibited commercial banks from offering investment banking and insurance services. The 1999 repeal of Glass-Steagall helped create the conditions in which banks created and invested in creative financial instruments such as mortgage-backed securities and credit default swaps, investment gambles that rocked the financial markets in 2008. More generally, the Depression-era conflicts and consequences that Glass-Steagall was intended to prevent re-emerged once the Act was repealed. The once staid commercial banking sector quickly evolved to emulate the risk-taking attitude and practices of investment banks, with disastrous results. "The most important consequence of the repeal of Glass-Steagall was indirect — it lay in the way repeal changed an entire culture," notes economist Joseph Stiglitz. "When repeal of Glass-Steagall brought investment and commercial banks together, the investment-bank culture came out on top. There was a demand for the kind of high returns that could be obtained only through high leverage and big risk taking."[42]

Unregulated Financial Derivatives. The 2008 crash proved Warren Buffet's warning that financial derivatives represent "weapons of mass financial destruction" to be prescient.[43] Financial derivatives amplified the financial crisis far beyond the troubles connected to the popping of the housing bubble. AIG made aggressive bets on credit default swaps (CDSs) that went bad with the housing bust, and led to a taxpayer-financed rescue of more than $130 billion. AIG was able to put itself at such risk because its CDS business was effectively subject to no governmental regulation or even oversight. That was because first, high officials in the Clinton administration and the Federal Reserve, including SEC Chair Arthur Levitt, Treasury Secretary Robert Rubin, Deputy Treasury Secretary Lawrence Summers and Federal Reserve Chair Alan Greenspan, blocked the Commodity Futures Trading Commission (CFTC) from regulating financial derivatives;[44]

---

[40] Tyson, J., Torres, C., & Vekshin, A. (2007, March 22). *Fed Says It Could Have Acted Sooner on Subprime Rout*. Bloomberg. Available at: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a1.KbcMbvIiA&refer=home.

[41] Torres, C., & Vekshin, A. (2007, March 14). *Fed, OCC Publicly Chastised Few Lenders During boom*. Bloomberg. Available at: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a6WTZifUUH7g&refer=us.

[42] Stiglitz, J. (2009). Capitalist fools. *Vanity Fair, 51*(1).

[43] Buffett, W. (2003). *Report to Shareholders, February 21, 2003*. Berkshire Hathaway. Available at: http://www.berkshirehathaway.com/letters/2002pdf.pdf.

[44] After the collapse of Long-Term Capital Management, Born issued a new call to regulate financial derivatives. "This episode should serve as a wake-up call about the unknown risks that the over-the-counter derivatives market may pose to the U.S. economy and to financial stability around the world," Born told the House Banking Committee two days later. "It has highlighted an immediate and pressing need to address whether there are unacceptable regulatory gaps relating to hedge funds and other large OTC derivatives market participants." But what should have been a moment of vindication for Born was swept aside by her adversaries, and Congress enacted a six-month moratorium on any CFTC action regarding derivatives or the swaps market. In May 1999, Born resigned in frustration. Born, B. (1998). *Testimony of Brooksley Born, Chairperson, Commodity Futures Trading Commission*

and second, because Congress and President Clinton codified regulatory inaction with passage of the Commodity Futures Modernization Act, which enacted a statutory prohibition on CFTC regulation of financial derivatives.

The SEC's Voluntary Regulation Regime for Investment Banks. In 1975, the SEC's trading and markets division promulgated a rule requiring investment banks to maintain a debt-to-net capital ratio of less than 12 to 1. It forbade trading in securities if the ratio reached or exceeded 12 to 1, so most companies maintained a ratio far below it. In 2004, however, the SEC succumbed to a push from the big investment banks — led by Goldman Sachs and its then-chair, Henry Paulson — and authorized investment banks to develop their own net capital requirements in accordance with standards published by the Basel Committee on Banking Supervision. This essentially involved complicated mathematical formulas that imposed no real limits, and was voluntarily administered. With this new freedom, investment banks pushed borrowing ratios to as high as 40 to 1, as in the case of Merrill Lynch. This super-leverage not only made the investment banks more vulnerable when the housing bubble popped, it enabled the banks to create a more tangled mess of derivative investments — so that their individual failures, or the potential of failure, became systemic crises. On September 26, 2008, as the crisis became a financial meltdown of epic proportions, SEC Chair Christopher Cox, who spent his entire public career as a deregulator, conceded "the last six months have made it abundantly clear that voluntary regulation does not work."[45]

Poorly Regulated Credit Ratings Firms. The credit rating firms enabled pension funds and other institutional investors to enter the securitized asset game, by attaching high ratings to securities that actually were high risk, as subsequent events revealed. The credit ratings firms have a bias toward offering favorable ratings to new instruments because of their complex relationships with issuers,[46] and their desire to maintain and obtain other

---

Concerning Long-Term Capital Management Before the U.S. House of Representatives Committee on Banking and Financial Services. Available at: http://www.cftc.gov/opa/speeches/opaborn-35.htm.

[45] Faoila, A., Nakashima, E., & Drew, J. (2008, October 15). *What Went Wrong*. The Washington Post. Available at: www.washingtonpost.com/wp-dyn/content/story/2008/10/14/ST2008101403344.html.

[46] The CEO of Moody's reported in a confidential presentation that his company is "continually 'pitched' by bankers" for the purpose of receiving high credit ratings and that sometimes "we 'drink the Kool-Aid.'" A former managing director of credit policy at Moody's testified before Congress that, "Originators of structured securities [e.g., banks] typically chose the agency with the lowest standards," allowing banks to engage in "rating shopping" until a desired credit rating was achieved. The agencies made millions on mortgage-backed securities ratings and, as one member of Congress said, "sold their independence to the highest bidder." Banks paid large sums to the ratings companies for advice on how to achieve the maximum, highest quality rating. "Let's hope we are all wealthy and retired by the time this house of cards falters," a Standard & Poor's employee candidly revealed in an internal email obtained by congressional investigators.

Other evidence shows that the firms adjusted ratings out of fear of losing customers. For example, an internal email between senior business managers at one of the three ratings companies calls for a "meeting" to "discuss adjusting criteria for rating CDOs [collateralized debt obligations] of real estate assets this week because of the ongoing threat of losing deals." In another email, following a discussion of a competitor's share of the ratings market, an employee of the same firm states that aspects of the firm's ratings methodology would have to be revisited in order to recapture market share from the competing firm.

See Weissman, R., & Donahue, J. (2009, March). *Sold Out: How Wall Street and Washington Betrayed America*. Essential Information and Consumer Education Foundation. Available at: http://wallstreetwatch.org/reports/sold_out.pdf.

> business dealings from issuers. This institutional failure and conflict of interest might and should have been forestalled by the SEC, but the Credit Rating Agencies Reform Act of 2006 gave the SEC insufficient oversight authority. In fact, under the Act, the SEC was required to give an approval rating to credit ratings agencies if they adhered to their own standards — even if the SEC knew those standards to be flawed.

The regulatory failure story can perhaps be summarized as follows: Financial deregulation and non-regulation created a vicious cycle that helped inflate the housing bubble and an interconnected financial bubble. Weak mortgage regulation enabled the spread of toxic and predatory mortgages that helped fuel the housing bubble. Deregulated Wall Street firms and big banks exhibited an insatiable appetite for mortgage loans, irrespective of quality, thanks to insufficiently regulated securitization, off-the-books accounting, the spread of shadow banking techniques, dangerous compensation incentives and inadequate capital standards. Reckless financial practices were ratified by credit ratings firms, paving the way for institutional funders to pour billions into mortgage-related markets; and an unregulated derivatives trade offered the illusion of systemic insurance but actually exacerbated the crisis when the housing bubble popped and Wall Street crashed.

To prevent the collapse of the financial system, the federal government provided incomprehensibly huge financial supports, far beyond the $700 billion in the much-maligned Troubled Assets Relief Program (TARP). The Special Inspector General for the Troubled Assets Relief Program (SIGTARP) estimated that "though a huge sum in its own right, the $700 billion in TARP funding represents only a portion of a much larger sum — estimated to be as large as $23.7 trillion — of potential Federal Government support to the financial system."[47] Much of this sum was never allocated, and most of the TARP funds were paid back. However, the regulatory reform policy debate should acknowledge that such unfathomable sums were put at risk thanks to regulatory failure.

Even more significant, however, are the actual losses traceable to the regulatory failure-enabled Great Recession. These losses are real, not potential; they are at a comparable scale of more than $20 trillion; they involve an actual loss of economic output, not just a reallocation of resources; and they have imposed devastating pain on families, communities and national well-being.

A GAO study found that "[t]he 2007-2009 financial crisis, like past financial crises, was associated with not only a steep decline in output but also the most severe economic downturn since the Great Depression of the 1930s."[48] Reviewing estimates of lost economic output, GAO reported that the present value of cumulative output losses could exceed $13 trillion.[49] Additionally, GAO found that "households collectively lost about $9.1 trillion (in constant 2011

---

[47] Special Inspector General for the Troubled Assets Relief Program (SIGTARP) (2009, July 21.) *Quarterly Report to Congress*. p. 129. Available at: http://www.sigtarp.gov/Quarterly%20Reports/July2009_Quarterly_Report_to_Congress.pdf.

[48] U.S. Government Accountability Office. (2013, Jan. 13). *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act*. p. 12. Available at: http://www.gao.gov/products/GAO-13-180.

[49] *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act*. p. 16.

dollars) in national home equity between 2005 and 2011, in part because of the decline in home prices."[50]

The recession threw millions out of work, and left millions still jobless or underemployed. "The monthly unemployment rate peaked at around 10 percent in October 2009 and remained above 8 percent for over 3 years, making this the longest stretch of unemployment above 8 percent in the United States since the Great Depression," GAO noted.[51]

The economic impact on families is crushing, even leaving aside social and psychological consequences. "Displaced workers — those who permanently lose their jobs through no fault of their own — often suffer an initial decline in earnings and also can suffer longer-term losses in earnings," reports GAO. For example, one study found that workers displaced during the 1982 recession earned 20 percent less, on average, than their non-displaced peers 15 to 20 years later.[52] Thanks to lost income and especially collapsed housing prices, families have seen their net worth plummet. According to the Federal Reserve's Survey of Consumer Finances, median household net worth fell by $49,100 per family, or by nearly 39 percent, between 2007 and 2010.[53]

The foreclosure crisis stemming from the toxic brew of collapsing housing prices, exploding and other unsustainable mortgages and high unemployment has devastated families and communities across the nation.[54]

There are, to be sure, dissenting views to narratives that place regulatory failure at the core of the explanation for the Great Recession and financial crisis. Perhaps the most eloquent version of this dissent is contained in the primary dissenting statement to the Financial Crisis Inquiry Commission.

The dissent explained that "we … reject as too simplistic the hypothesis that too little regulation caused the Crisis,"[55] arguing that the *amount* of regulation is an imprecise and perhaps irrelevant metric. This is a reasonable position (and it applies equally to those who complain about "too much" regulation); what matters is the quality of regulation — both the rules and standards of enforcement.

---

[50] *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act.* p. 21. There is necessarily a significant amount of uncertainty around such analyses. Other estimates have placed the loss somewhat lower. A recent Congressional Budget Office study estimates the cumulative loss from the recession and slow recovery at $5.7 trillion." (Congressional Budget Office. 2012. *The Budget and Economic Outlook: Fiscal Years 2012 to 2022.* p. 26.) One complicating issue is determining which losses should be attributed to the recession and which to other issues. For example, GAO notes, "analyzing the peak-to-trough changes in certain measures, such as home prices, can overstate the impacts associated with the crisis, as valuations before the crisis may have been inflated and unsustainable.[50] *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act.* p. 17.

[51] *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act.* pp. 17-18.

[52] *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act.* pp. 18-19.

[53] Cited in *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act.* p. 16.

[54] *Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act.* pp. 23-24.

[55] *The Financial Crisis Inquiry Report.* (Dissenting Views By Keith Hennessey, Douglas Holtz-Eakin, and Bill Thomas.) p. 414.

The FCIC dissent began its explanation for the financial crisis with the creation of a credit bubble and a housing bubble, which it argued laid the groundwork for a financial crisis thanks to a series of other, interconnected factors, including the spread of nontraditional mortgages, securitization, poor functioning by credit rating firms, inadequate capitalization by financial firms, the amplification of housing bets through use of synthetic credit derivatives, and the risk of contagion due to excessive interconnectedness.

However, to review this list is to see how the FCIC dissent also implicitly argued that the crisis can be blamed in large part on regulatory failure. For all of these factors should have been tamed by appropriate regulatory action.

The Congressional response to the financial crisis, of course, was passage of the Dodd-Frank Act. Few people are entirely satisfied with the Dodd-Frank legislation — Public Citizen is highly critical of a number of important omissions — but the Act does include an array of very important reforms that will make our financial system fairer and more stable, if properly implemented through robust rulemaking.

Rolling back or diluting those measures – as Wall Street now seeks to do, away from the glare of public attention — is to invite yet another financial meltdown.

B. The Ongoing Need for Regulation in the Financial Sector

Although the 2008 financial crash and Great Recession was (hopefully) a once-in-a-lifetime event, abuses in the financial sector remain rampant, illustrating the need for stronger regulation and tougher regulatory enforcement. Two recent, notable debacles – Wells Fargo's fake account scandal and a series of other serious abuses, and the Equifax data breach – should put to rest the notion that the financial sector is overburdened with duplicative or unfair rules.

Wells Fargo: In September 2016, the Consumer Financial Protection Bureau (CFPB), [56] the Office of the Comptroller of the Currency (OCC),[57] and the Los Angeles (LA) City Attorney[58] fined Wells Fargo $185 million for engaging in fraudulent cross-selling practices.[59] Wells Fargo neither admitted nor denied wrongdoing.

In August 2017, a year after the initial penalty announcement, a review of Wells Fargo activities going back to 2009 found additional fraudulent accounts, bringing the total number of reported

---

[56] Wells Fargo consent order, U.S. Consumer Financial Protection Bureau (Sept. 8, 2016), available at: https://files.consumerfinance.gov/f/documents/092016_cfpb_WFBconsentorder.pdf.

[57] Wells Fargo consent order, U.S. Office of the Comptroller of the Currency, (Sept. 8, 2016), available at: https://occ.gov/news-issuances/news-releases/2016/nr-occ-2016-106b.pdf.

[58] Press release, "Los Angeles City Attorney Mike Feuer Achieves Historic Result in Consumer Action Against Wells Fargo; Bank to Make Restitution to Customers, Pay $50-million in Penalties; Unprecedented Coordination with Federal Regulators to Benefit Consumers Nationwide," Los Angeles City Attorney (Sept. 8, 2016), available at: https://www.lacityattorney.org/single-post/2016/09/08/Los-Angeles-City-Attorney-Mike-Feuer-Achieves-Historic-Result-in-Consumer-Action-Against-Wells-Fargo-Bank-to-Make-Restitution-to-Customers-Pay-50-million-in-Penalties-Unprecedented-Coordination-with-Federal-Regulators-to-Benefit-Consumers-Nationwide.

[59] Michael Tanglis, "The "King of Cross-Sell" and the Race to Eight," Public Citizen (Sept. 29, 2016), available at: https://www.citizen.org/sites/default/files/wells-fargo-king-of-cross-sell.pdf.

fake accounts up to 3.5 million.[60] As a result, 190,000 related accounts incurred fees. Wells Fargo pledged to refund consumers a total of $6.1 million in wrongful charges plus interest.[61] Wells Fargo also paid $3.7 million to address further complaints and settled a $142 million class action lawsuit brought on behalf of wronged consumers.[62]

5,300 employees were fired for the alleged wrongdoing.[63] Fallout from the scandal included allegations the bank fired whistleblowers; OSHA ordered the bank to pay one whistleblower $5.4 million and required that he be rehired.[64] (About 2,000 were later hired back.)[65] The board ousted CEO John Stumpf in the fallout and executive Carrie Tolstedt was retroactively terminated after her retirement. Each lost over $60 million in compensation and clawbacks.[66]

Then-CFPB Director Richard Cordray said, "Today's enforcement actions against Wells Fargo likely could have been prevented if the bank had a stronger compliance risk management program that fostered a more healthy culture, in which incentives aligned behaviors properly."[67] Stumpf reportedly was aware of problems with the bank's cross-selling practices as far back as 2002.[68] A detailed report by Wells Fargo's board of directors identifies executive failures and the bank's "decentralized"[69] structure as factors that permitted the crisis to occur.

Among the report's principal findings:[70]

---

[60] Press release, "Wells Fargo Reports Completion of Expanded Third-Party Review of Retail Banking Accounts, Paving Way to Complete Remediation Effort," Wells Fargo (Aug. 31, 2017), available at: https://newsroom.wf.com/press-release/wells-fargo-reports-completion-expanded-third-party-review-retail-banking-accounts.

[61] *Ibid.*

[62] James Rufus Koren, "Wells Fargo's $142-million sham accounts settlement: What you need to know," Los Angeles Times (July 11, 2017), available at: http://www.latimes.com/business/la-fi-wells-fargo-settlement-20170710-htmlstory.html.

[63] Renae Merle, "Wells Fargo boots 5,300 employees for creating accounts its customers didn't ask for," The Washington Post (Sept. 8, 2016), available at: https://www.washingtonpost.com/news/business/wp/2016/09/08/wells-fargo-fined-185-million-for-creating-accounts-its-customers-didnt-ask-for.

[64] Stacy Cowley, "Wells Fargo Whistle-Blower Wins $5.4 Million and His Job Back," The New York Times (April 3, 2017), available at: https://www.nytimes.com/2017/04/03/business/04-wells-fargo-whistleblower-fired-osha.html.

[65] Patrick Rucker, "Wells Fargo rehires workers pushed aside in accounts scandal," Reuters (Oct. 2, 2017), available at: https://www.reuters.com/article/us-wells-fargo-accounts-sloan/wells-fargo-rehires-workers-pushed-aside-in-accounts-scandal-idUSKCN1C721S.

[66] Wilfred Frost and Dawn Giel, "Wells Fargo board slams former CEO Stumpf and Tolstedt, claws back $75 million," CNBC (April 10, 2017), available at: https://www.cnbc.com/2017/04/10/wells-fargo-board-slams-stumpf-and-tolstedt-claws-back-millions.html.

[67] Renae Merle, "Wells Fargo boots 5,300 employees for creating accounts its customers didn't ask for," The Washington Post (Sept. 8, 2016), available at: https://www.washingtonpost.com/news/business/wp/2016/09/08/wells-fargo-fined-185-million-for-creating-accounts-its-customers-didnt-ask-for.

[68] Wilfred Frost and Dawn Giel, "Wells Fargo board slams former CEO Stumpf and Tolstedt, claws back $75 million," CNBC (April 10, 2017), available at: https://www.cnbc.com/2017/04/10/wells-fargo-board-slams-stumpf-and-tolstedt-claws-back-millions.html.

[69] Independent Directors of the Board of Wells Fargo & Company, "Sales Practices Investigation Report," Wells Fargo (April 10, 2017), available at: https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/presentations/2017/board-report.pdf.

[70] *Ibid.*

> Corporate control functions were constrained by the decentralized organizational structure and a culture of substantial deference to the business units. In addition, a transactional approach to problem-solving obscured their view of the broader context. As a result, they missed opportunities to analyze, size and escalate sales practice issues. Sales practices were not identified to the Board as a noteworthy risk until 2014. By early 2015, management reported that corrective action was working. Throughout 2015 and 2016, the Board was regularly engaged on the issue; however, management reports did not accurately convey the scope of the problem. The Board only learned that approximately 5,300 employees had been terminated for sales practices violations through the September 2016 settlements with the Los Angeles City Attorney, the OCC and the CFPB.

As a result of Wells Fargo's compliance failures, the bank has been subsequently penalized for multiple regulatory violations,[71] including the remarkable sanction of having its growth capped by the Federal Reserve[72] because of its consumer failures and a $1 billion penalty from the CFPB and OCC for overcharging consumers with mortgage fees and charging about 2 million consumers for "duplicative or unnecessary" insurance policies.[73]

Equifax: In 2017, hackers accessed and stole sensitive data held by Equifax about more than 146.6 million Americans.[74] The data Equifax accessed includes individuals' full names, birth dates, Social Security numbers, driver's license numbers and credit card information. It was the second-largest hack of this kind, second only to Yahoo.[75]

It bears reminding that ordinary Americans are not Equifax's customers – individuals' information is Equifax's product, which they collect and sell to banks.

The Equifax attack occurred on May 13. Six weeks lapsed between Equifax becoming aware of the attack and the attack being made public on September 7.[76] For months, the credit-rating company failed to disclose the full extent of the breach.[77]

---

[71] "Wells Fargo," Violation Tracker database (accessed July 6, 2018), available at: https://violationtracker.goodjobsfirst.org/parent/wells-fargo.

[72] "Responding to widespread consumer abuses and compliance breakdowns by Wells Fargo, Federal Reserve restricts Wells' growth until firm improves governance and controls. Concurrent with Fed action, Wells to replace three directors by April, one by year end," Board of Governors of the Federal Reserve System (Feb, 2, 2018), available at: https://www.federalreserve.gov/newsevents/pressreleases/enforcement20180202a.htm.

[73] Wells Fargo consent order, U.S. Consumer Financial Protection Bureau (April 20, 2018), available at: https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-bank-na_consent-order_2018-04.pdf.

[74] "Equifax's Statement for the Record Regarding the Extent of the Cybersecurity Incident Announced on September 7, 2017," U.S. Securities and Exchange Commission form EX-99.1 (May 8, 2018), available at: https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm.

[75] AnnaMaria Androitis, "Equifax Customer Complaints Continue to Pile Up," Fox Business (Sept. 10, 2017), available at: https://www.foxbusiness.com/features/equifax-customer-complaints-continue-to-pile-up.

[76] Michael Rapoport and AnnaMaria Andriotis, "States Push Equifax to Explain Why It Took 6 Weeks to Disclose Hack," Fox Business (Sept. 10, 2017), available at: https://www.wsj.com/articles/states-push-equifax-to-explain-why-it-took-6-weeks-to-disclose-hack-1509196933.

[77] AnnaMaria Andriotis, "Equifax Hack Might Be Worse Than You Think," The Wall Street Journal (Feb. 9, 2018), available at: https://www.wsj.com/articles/equifax-hack-might-be-worse-than-you-think-1518191370.

CEO Richard Smith was aware of the attack for three weeks before it was made public.[78] A report by the office of Senator Elizabeth Warren (D-Mass.) notes that, "By failing to provide adequate information in a timely fashion, Equifax robbed consumers of the ability to take precautionary measures to protect themselves."[79]

Equifax bungled the immediate fallout of the hack disclosure – customer help lines and websites were unresponsive to the massive demand for assistance,[80] and the company for a time required consumers to agree to a forced arbitration clause that would deny their right to hold it accountable in court.[81] Public outrage forced the company to drop its rip-off clause for remedial services provided.[82]

For months, the credit-rating company failed to disclose the full extent of the breach.[83] So far, an executive and a software engineering manager have been charged with insider trading on information about the hack before the news was public.[84] State regulatory agencies have imposed new data security requirements on Equifax, but no penalties have been levied.[85] Reuters has reported that acting CFPB director Mick Mulvaney has so far declined to investigate Equifax.[86] The FTC is investigating, and a class-action lawsuit against the company is being pursued by all 50 states and the District of Columbia.[87] The IRS temporarily suspended its $7.2 million contract with Equifax to verify taxpayer identities.[88]

However, the combination of the Trump administration's hostility to regulatory enforcement and the completely inadequate privacy protection regulatory framework means that Equifax may

---

[78] Chris Arnold, "Equifax CEO Richard Smith Resigns After Backlash Over Massive Data Breach," National Public Radio (Sept. 26, 2017), available at: https://www.npr.org/2017/09/26/553799200/equifax-ceo-richard-smith-resigns-after-backlash-over-massive-data-breach.

[79] "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information," Office of Senator Elizabeth Warren (Feb. 2018), available at: https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf.

[80] AnnaMaria Androitis, "Equifax Customer Complaints Continue to Pile Up," Fox Business (Sept. 10, 2017), available at: https://www.foxbusiness.com/features/equifax-customer-complaints-continue-to-pile-up.

[81] Mahita Gajanan, "Equifax Says You Won't Surrender Your Right to Sue by Asking for Help After Massive Hack," TIME (Sept. 11, 2017), available at: http://time.com/4936081/equifax-data-breach-hack.

[82] Press release, "Equifax Removes Rip-Off Clause, Backing Down Under Pressure From Consumers," Public Citizen (Sept. 11, 2017), available at: https://www.citizen.org/media/press-releases/equifax-removes-rip-clause-backing-down-under-pressure-consumers.

[83] AnnaMaria Andriotis, "Equifax Hack Might Be Worse Than You Think," The Wall Street Journal (Feb. 9, 2018), available at: https://www.wsj.com/articles/equifax-hack-might-be-worse-than-you-think-1518191370.

[84] Tara Siegel Bernard, "Another Equifax Employee Faces Charge of Insider Trading After Big Breach," The New York Times (June 28, 2018), available at: https://www.nytimes.com/2018/06/28/business/equifax-insider-trading-sec.html.

[85] Kate Fazzini, "Equifax gets new to-do list, but no fines or penalties," CNBC (June 27, 2018), available at: https://www.cnbc.com/2018/06/27/equifax-breach-consent-order-issued.html.

[86] Patrick Rucker, "Exclusive: U.S. consumer protection official puts Equifax probe on ice - sources," Reuters (Feb. 5, 2018), available: https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ.

[87] Tara Swaminatha, "Equifax now hit with a rare 50-state class-action lawsuit," CSO Online (Nov. 22, 2017), available at: https://www.csoonline.com/article/3238076/data-breach/equifax-now-hit-with-a-rare-50-state-class-action-lawsuit.html.

[88] Steven Overly, "IRS temporarily suspends contract with Equifax," Politico (Oct. 12, 2017), available at: https://www.politico.com/story/2017/10/12/irs-equifax-contract-suspended-243732.

escape full accountability – an accountability failure that will encourage rather than deter other companies from the same lax security, reporting sloth and inadequate remedies that Equifax displayed.

C. Deregulation Injuring Consumers and the Planet: Clean Car Standards

The Trump administration's roll back of vehicle fuel efficiency standards is one of the worst deregulatory decisions in history. Where other deregulatory disasters could at least be justified at the decision point based on fanciful claims that they would create no undue risk and generate economic savings, the roll back of the clean car standard fails utterly and totally on both accounts. It will dramatically worsen climate pollution, speeding our rush to climate catastrophe. At the same time, not only will it introduce massive regulatory uncertainty for auto makers, it will cost consumers, and the national economy, hundreds of billions of dollars. It's not easy to make a decision this bad.

In 2011, automakers, labor groups and environmentalists stood in the Rose Garden beside President Barack Obama as he announced national clean car standards. The standards were the product of a negotiation among the National Highway Traffic Safety Administration (NHTSA), the Environmental Protection Agency (EPA), the California Air Resources Board (CARB), the auto makers and others. Together, they agreed that the auto industry could catapult forward to meet "One National Program," making much more efficient vehicles, aiding the industry, protecting the planet and providing dramatic savings to consumers.[89]

The joint standards were issued in phases. In 2010, standards were finalized for model years (MY) 2012-2016. In 2012, standards were promulgated for MY 2017-2025.[90] The clean car regulations finalized in 2012 provided for a "midterm review" of the appropriateness of standards established for model years 2022-25. In January 2017, the EPA issued a final determination that the standards were appropriate and would remain unchanged: "At every step in the process the analysis has shown that the greenhouse gas emissions standards for cars and light trucks remain affordable and effective through 2025, and will save American drivers billions of dollars at the pump while protecting our health and the environment."[91]

Those gains now are threatened because, since President Donald Trump's election and despite having helped craft the clean car standards, automakers have pushed to roll them back. In April 2018, the EPA reversed the January 2017 final determination, requiring the agency to promulgate new standards for MY 2021-2025. Public Citizen and other organizations have petitioned to reverse that decision, as have numerous states.[92] The EPA and NHTSA are

---

[89] https://obamawhitehouse.archives.gov/the-press-office/2012/08/28/obama-administration-finalizes-historic-545-mpg-fuel-efficiency-standard

[90] The standards require the fleet average for each manufacturer to be 163 grams CO2e emitted per mile, or 54.5 mpg when translated into fuel economy

[91] Midterm Evaluation of Light-Duty Vehicle Greenhouse Gas Emissions Standards for Model Years 2022-2025, U.S. Environmental Protection Agency. Available at: https://www.epa.gov/regulations-emissions-vehicles-and-engines/midterm-evaluation-light-duty-vehicle-greenhouse-gas

[92] Center for Biological Diversity; Conservation Law Foundation; Environmental Defense Fund; Natural Resources Defense Council; Public Citizen, Inc.; Sierra Club, and Union of Conerned Scientists v. United States

expected to introduce alternative standards, vastly inferior to those already agreed upon, and likely eviscerating California's historic right to establish fuel efficiency standards more aggressive than federal rules require.

According to leaked documents, the rollback would result in:[93]

- Emission of an additional 2.2 billion metric tons of global warming pollution that would have been avoided by 2040.
- Burning 200 billion more gallons of fuel by 2040, the equivalent of 1.5 years of U.S. oil production.
- Consumers wasting hundreds of billions of dollars in excess spending at the pump.

The EPA and NHTSA's decision is a reflexive, ideological and industry-driven maneuver, not supported by scientific evidence, [94] cost accounting, industry's long-term interest, respect for the agency's public health and environmental mission or consideration of consumers' economic interest.

In stark contrast to the industry's expressed and real desire for regulatory certainty and a single national standard, the EPA and NHTSA's deregulatory action will launch years of confusion for the industry. If the EPA and NHTSA undermine the federal program, California and the states that follow California's standard – making up one third of the new vehicle market – will maintain their own higher standards, upsetting the goal of a single national standard.[95] If EPA and NHTSA seek to override California's historic right to establish a stronger standard, its action will be tied up in court for years. Indeed, the revocation of the clean car standards itself is likely to be tied up in litigation for years – leaving auto makers uncertain of future requirements and, more importantly, without the incentive to invest quickly in fuel efficient cars that would advance public health, save consumers and help avert catastrophic climate change.

What makes the EPA and NHTSA's move so startling is not just that it ignores environmental imperatives, but that this is a case where environmental protection is perfectly aligned with consumer and national economic interest. The fuel efficiency standards that the administration aims to cancel would generate dramatic savings for consumers. With the existing EPA standards, when compared to a typical vehicle on the road today, a new car buyer will save about $3,200-$5,700 over the lifetime of a new 2025 car, even after considering the cost of more fuel-efficient technology and lower gasoline prices. New truck buyers will save even more — about $4,800-

---

Environmental Protection Agency, Petition for Review. Available at: https://www.citizen.org/sites/default/files/ngo_petition_for_review_of_revised_fd_final_5-15-18.pdf

[93] Tom Carper, Letter to Elaine Chao and Scott Pruitt, May 1, 2018. Available at: https://www.epw.senate.gov/public/_cache/files/7/2/72b2d596-d456-483a-8c8a-ba4bfea4a145/BE7A29D9A17B01162A7DA6FEE7C2A0BA.05012018-carper-letter-chao-pruitt-draft-fuel-economy-tailpipe-emissions.pdf

[94] Dave Cooke, "EPA Pulls Back Sound Policy Judgment at Behest of Auto Industry", Union of Concerned Scientists, March 15, 2017. Available at: https://blog.ucsusa.org/dave-cooke/epa-pulls-back-sound-policy-judgment-at-behest-of-auto-industry

[95] Timothy Gardner, U.S. States Vow to Defend Auto Fuel Efficiency Standards, Reuters, April 3, 2018, available at: https://www.reuters.com/article/us-usa-epa-autos/u-s-states-vow-to-defend-auto-fuel-efficiency-standards-idUSKCN1HA2DI

$8,200 over the lifetime of a new 2025 truck.[96] With Americans buying roughly 17 million cars a year, the savings will quickly total in the hundreds of billions of dollars. These are savings both to consumers and the national economy — lost if the Trump administration has its way.

D. Deregulation Striking at the American Dream: Protections for Victims of Predatory Student Loans

Student debt is a national crisis, with students owing more than $1.5 trillion in total.[97] Some of this debt is surely unpayable, including debt held by students who borrowed heavily from the federal government to receive inadequate post-secondary education, overwhelmingly from for-profit schools. The Trump administration's deregulation in this area will leave tens of thousands of students in debt for decades or more and at the mercy of unchecked private student loan servicers. This will shamefully and needlessly damage borrowers' life prospects – a disgraceful regulatory failure to benefit politically connected rip-off institutions at the expense of young (and not-so-young) adults whose only sin was investing in what they believed to be a legitimate educational pathway to achieve the American Dream.

The Higher Education Act of 1965 establishes that student loan borrowers can have their federal Direct Loans discharged (through a process known as "borrower defense") if their schools have engaged in certain types of unlawful conduct with respect to the borrowers' education. However, the first set of debt-relief regulations implementing this statutory provision were not established until 1995 and those rules did not set out a clear process for students to submit claims for debt relief. As a result, only five borrowers submitted claims from the mid-1990s until an unprecedented wave of debt-relief claims began in 2015 after the collapse of some for-profit colleges.[98]

Under the Obama administration, the Education Department attempted to improve and clarify the debt-relief process, finalizing new rules in November 2016. Those rules also imposed accountability and other measures designed to discourage school misconduct and protect students. They provided, for example, for a clearer process by which the federal government could recoup from predatory schools the cost of loan discharges through the borrower defense process. They also prohibited the flow of some federal loan assistance to schools that use or enforce forced arbitration clauses with their students to evade liability when the schools break the law.

However, Secretary of Education Betsy DeVos, has blocked this 2016 rule from going into effect, presumably reflecting her view that it would be unfair to for-profit schools ripping off young adults seeking educational opportunity. "While students should have protections from predatory practices, schools and taxpayers should also be treated fairly as well," DeVos has said.

---

[96] Comings, A., A. Allison and F. Ackerman. 2016. Fueling savings: Higher fuel economy standards result in big savings for consumers. Available at: consumersunion.org/wp-content/uploads/2016/09/Fueling-Saving-Consumer-Savings-from-CAFE-2025.pdf,

[97] Jillian Berman, Student Debt Just Hit $1.5 Trillion, May 12, 2018, Marketwatch, available at: https://www.marketwatch.com/story/student-debt-just-hit-15-trillion-2018-05-08.

[98] Laura Feiveson, Alvaro Mezza, and Kamila Sommer, Student Loan Debt and Aggregate Consumption Growth, March 1, 2018, Federal Reserve, available at: https://www.federalreserve.gov/econres/notes/feds-notes/student-loan-debt-and-aggregate-consumption-growth-20180221.htm.

She claims the borrower defense process provided by the 2016 rule would wrongly give "free money" to victimized students.[99]

Public Citizen and the Project on Predatory Student Lending are suing the Department of Education to force implementation of the 2016 rule.[100] We represent two former students misled by a for-profit college who are seeking relief from their federal loans and the ability to sue their school in court despite the school's use of forced arbitration clauses.[101] Democratic attorneys general have also sued to prevent the 2016 borrower defense regulation from being delayed.[102] The Department of Education is expected to propose a far weaker, alternative rule this summer.

For-profit colleges prey upon disadvantaged populations. To a considerable extent, it is working students — veterans, single moms and minorities – who attend and are defrauded by for-profit colleges, as seen in stories of shoddy educational programs collected by U.S. Senate Democrats in a report published in November 2017.[103] Some examples:

> *"I wasted two years and a half of my life. They didn't even say that I will be in debt after graduation. At the beginning they told me not to worry about having a loan because I was eligible for the highest financial aid. The whole thing was just a blur... The two years and a half of my life were all lies."*
>
> — Nino, ITT Technical Institute

> *"I took out loans for a quality education and that is not what I got...the closest I worked [to interior design] was an internship for a guy who ended up being a druggie who had a cabinet shop."*
>
> — Heather Drattlo, The Art Institute of Indianapolis

> *"I was excited, breaking my back, staying up late, and carrying all these books around, taking notes, for what? For nothing. At the end of the day all we end up with is debt."*
>
> — Erika C., Everest College

---

[99] Jaqueline Thomsen, *DeVos: Victims of for-profit colleges just had to raise hands to get 'free money'*, The Hill, Sept. 25, 2017, http://thehill.com/homenews/administration/352264-devos-students-defrauded-by-for-profit-colleges-just-had-to-raise.

[100] *Bauer v. DeVos*, Available at: https://www.citizen.org/our-work/litigation/cases/bauer-v-devos.

[101] Public Citizen, Public Citizen and Project on Predatory Student Lending Represent Students Suing to Stop Education Department's Illegal Delay (July 6, 2017), http://bit.ly/2u2cnQP; Public Citizen, Public Citizen and Project on Predatory Student Lending Intervene in Suit To Protect Students Victimized by Predatory Schools (June 15, 2017), http://bit.ly/2tO5zGh.

[102] Michael Martin, 19 Attorneys General Sue DeVos over Delay of Borrower Defense Rule, NPR, All Things Considered, July 8, 2017, Available at: https://www.npr.org/2017/07/08/536197364/19-attorneys-general-sue-devos-over-delay-of-borrower-defense-rule

[103] Elizabeth Warren and Richard J. Durbin, "Insult to Injury: How the DeVos Department of Education is Failing Defrauded Students", United States Senate, November 2017. Available at: https://www.warren.senate.gov/files/documents/2017_11_Warren_Durbin_Borrower_Defense_Report.pdf

According to data obtained through a Freedom of Information Act request by the Century Foundation, more than 98 percent of the 128,000 borrower defense claims filed since 2015 involve for-profit colleges, with nearly 70 percent coming from Corinthian Colleges.[104] During the Obama administration, the Education Department approved nearly 32,000 borrower defense applications, even before the clearer borrower defense process set out in the 2016 rule was scheduled to take effect.

Although thousands more claims remained, under DeVos, the Education Department cut the number of workers processing borrower defense claims.[105] The Washington Post reported that top Education Department official James Manning directed staffers to stop sorting through students' debt relief claims and slashed the number of contractors working on those claims even as submissions kept piling up.[106] The Trump administration halted approvals until December 2017. That month, an inspector general's report called for the debt-relief process to resume[107] and four state attorneys general sued DeVos over the stalled relief claims.[108]

Shortly thereafter, the Education Department approved nearly 12,900 claims from Corinthian Colleges students but denied 8,600 claims.[109]

DeVos also shifted the Education Department's policy away from giving full debt relief to defrauded students. Instead, she granted partial debt relief to Corinthian Colleges students depending on student's average earnings.[110] Under this "partial relief" plan, borrowers who earn more money – even at low-wage retail jobs outside their field of study – would get less relief, while students with lower earnings or no income would get more help. Under this "tiered" debt relief system, Corinthian Colleges students have received relief levels as low as 10 percent rather than full relief.[111] Consumer lawyers are challenging the legality of the government's plan in court, arguing that students are entitled to full relief, and that the Education Department's tiered relief system would treat Corinthian students far worse than students from that schools who

---

[104] Yan Cao, Tariq Habash, "College Fraud Claims Up 29 Percent Since August 2017", The Century Foundation, May 20, 2018, Available at: https://tcf.org/content/commentary/college-fraud-claims-29-percent-since-august-2017/

[105] Danielle Douglas-Gabriel, *Trump administration undermined student debt relief unit while claims mounted, watchdog finds*," Wash. Post (June 14, 2018), https://wapo.st/2NoH2kA.

[106] Danielle Douglas-Gabriel, "Trump administration undermined student debt relief unit while claims mounted, watchdog finds" Washington Post (June 14, 2018) https://wapo.st/2NoH2kA.

[107] Office of Inspector General, "Federal Student Aid's Borrower Defense to Repayment Loan Discharge Process", U.S. Department of Education, December 8, 2017, Available at: https://www2.ed.gov/about/offices/list/oig/auditreports/fy2018/i04r0003.pdf.

[108] Danielle Douglas-Gabriel, Grade Point Betsy DeVos hit with two lawsuits in one day over backlog of student debt relief claims, The Washington Post, December 14, 2017. Available at: https://www.washingtonpost.com/news/grade-point/wp/2017/12/14/betsy-devos-hit-with-two-lawsuits-in-one-day-over-backlog-of-student-debt-relief-claims/?utm_term=.b624a8904c866

[109] Katie Lobosco, Betsy DeVos limits debt relief for defrauded students, CNN, December 21, 2017. Available at: http://money.cnn.com/2017/12/21/pf/college/devos-borrower-defense-debt-relief/index.html

[110] Erica L. Green, *For Students Swindled by Predatory Colleges, Relief May Only Be Partial*, N.Y. Times (Dec. 21, 2017), https://nyti.ms/2JffomE.

[111] U.S. Department of Education, "Borrower Defense Relief Methodology for CCI claims", U.S. Department of Education, December 15, 2017. Available at: https://www2.ed.gov/documents/press-releases/borrower-defense-relief-methodology-cci.pdf

already received relief under Obama.[112] Thankfully, the court has now ruled that the Education Department's partial relief plan violated federal privacy law.[113]

DeVos and the Trump administration also have made several other decisions that will hurt student loan borrowers:

- In response to state efforts to address student loan servicer abuses, the Education Department has advanced an interpretation of the Higher Education Act that would broadly preempt state consumer-protection measures.[114]
- The Trump administration decided to no longer protect student loan borrowers from collection fees if they enter into an agreement to repay their loans within two months of receiving a notice of default.[115] Trump's Education Department ended an agreement[116] to share consumer complaints about student loans and information about student loan payment collectors with the CFPB,[117] an arrangement that had benefited consumers by allowing both agencies to crack down on predatory institutions and to compensate students.
- The Education Department has sought to withdraw[118] an Obama administration decision to evaluate student-loan debt collectors' track records — including customer service standards — when deciding whether to award new contracts. This move may benefit problematic servicers who are trying to obtain lucrative government contracts.[119]

---

[112] Danielle Douglas-Gabriel, "Consumer lawyers want to end Education Department student debt relief plan", Washington Post, March 19, 2018. Available at: https://www.washingtonpost.com/news/grade-point/wp/2018/03/19/consumer-attorneys-want-to-put-an-end-to-education-dept-partial-student-debt-relief-plan/?utm_term=.51c844f72b10

[113] *Manriques v. Devos*, available at: https://predatorystudentlending.org/wp-content/uploads/2018/05/PI-Order.pdf.

[114] See Nate Raymond, "U.S. backs student loan servicer in lawsuit by Massachusetts", Reuters, January 10, 2018, Available at: https://www.reuters.com/article/us-massachusetts-education-lawsuit/u-s-backs-student-loan-servicer-in-lawsuit-by-massachusetts-idUSKBN1EZ210; Betsy DeVos, "Federal Preemption and State Regulation of the Department of Education's Federal Student Loan Programs and Federal Student Loan Services", Department of Education, March 1, 2018. Available at: https://s3.amazonaws.com/public-inspection.federalregister.gov/2018-04924.pdf.

[115] Lynn Mahaffie, Withdrawal of Dear Colleague Letter, United States Department of Education, March 16, 2017, Available at: https://ifap.ed.gov/dpcletters/attachments/GEN1702.pdf

[116] Sylvan Lane, "DeVos ends agreement to work on student loan fraud", The Hill, September 5, 2017. Available at: http://thehill.com/policy/finance/349223-education-dept-ends-agreement-to-work-with-consumer-bureau-on-student-loan

[117] Public disclosure that the information-sharing agreement had broken downtriggered a call by labor unions for a probe of potential insider-trading. See Pete Schroeder, AFL-CIO Wants SEC to Probe Trading in Shares of Loan Servicer Navient, October 10, 2017, available at: https://www.reuters.com/article/us-usa-sec-navient/afl-cio-wants-sec-to-probe-trading-in-shares-of-loan-servicer-navient-idUSKBN1CF2UV.

[118] Id.; Andrew Kreighbaum, "Student Aid And Loans Trump Administration Backs Off Reshuffling of Student Debt Collection", July 9, 2018. Available at: https://www.insidehighered.com/news/2018/07/09/after-rebuke-congress-education-department-suspends-reshuffling-defaulted-student

[119] Memo from Ted Mitchell, Under Secretary, U.S. Department of Education to James Runcie, Chief Operating Officer, Federal Student Aid, Re: Policy Direction on Federal Student Loan Servicing (July 20, 2016), http://bit.ly/2tKjDSV.

- The student loan giant Navient has been pressuring the Consumer Financial Protection Bureau (CFPB) to drop a lawsuit alleging mistreatment of student borrowers.[120] Given the CFPB's new leadership, it's fair to assume that these arguments are getting a receptive audience.

IV. Sectoral Issues Regarding Regulatory Duplication

In a complicated economy, with a vast federal bureaucracy, there will surely be regulatory overlap. A lot of this overlap will be purposeful and desirable, as different agencies advance different public purposes and protect diverse interests. There may be some instances where unnecessary regulatory duplication, or possibly even conflicting standards apply. However, despite Big Business assertions that such regulatory duplication is widespread, costly and wasteful, there is no evidence to support such claims. Some of what corporations are complaining about are purposeful overlapping regulatory standards; but it seems that claims of regulatory duplication primarily are dressed up complaints about regulation itself.

A. Cybersecurity and Privacy Protections

The United States is not adequately addressing cybersecurity issues. This is true of both the U.S. government and large corporate actors. If federal agencies are making overlapping demands of states or other entities, it may well reflect a patchwork problem – the absence of an overarching regulatory framework. On the other hand, some overlapping demands may well be justified – as consideration of the differential standards and requirements to protect election security, medical records and critical infrastructure illustrates.

If there are issues with duplicative or competing cybersecurity demands, most are likely best managed through an overarching, federal cybersecurity and internet privacy framework. Indeed, there is an urgent need for such a regulatory framework with the rise of the Internet of Things. The increasing connectivity of a wide range of products and devices – from automobiles to toasters – may offer consumer benefits from energy savings to product performance to safety. But in this new world, data breaches and lack of privacy safeguards pose new risks, threatening frightening automobile accidents, identity theft, improper marketing, racially discriminatory practices and much more.[121] The Equifax data breach – and the company's epic mishandling of the breach – provides only a tiny insight into the scope of the nascent threats.

---

[120] Michael Stratford, "Kennedy resignation could spark changes to affirmative action", Politico, June 28, 2018. Available at: https://www.politico.com/newsletters/morning-education/2018/06/28/kennedy-resignation-could-spark-changes-to-affirmative-action-266608

[121] Federal Trade Commission, Internet of Things, Privacy & Security in a Connected World, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Seeta Pena Gangadharan, ed., Data and Discrimination, Open Technology Institute/New America Foundation, 2014, available at: https://www.newamerica.org/oti/policy-papers/data-and-discrimination; Consumer Reports and Consumer Federation of America, Comments on Cybersecurity Best Practices for Modern Vehicles, November 28, 2016, available at: < https://consumersunion.org/wp-content/uploads/2016/11/CR-CU-comments-to-NHTSA-on-Cybersecurity-Best-Practices-11-28-2016.pdf>.

Against this backdrop, as well as the revelations of Cambridge Analytica's misuse of Facebook data – albeit in ways that reflect contemporary "Big Data" commercial targeting practices used by most large businesses – it is distressing that neither the Congress nor the administration have taken any significant steps toward adopting meaningful data and privacy protections. Indeed, the most consequential action has been Congress's misguided repeal of Federal Communication Commission rules that would have proposed minimal privacy standards on broadband providers. The rules had required Internet Service Providers to obtain affirmative consent before collecting consumers' personal information – including browser history – and making it available to third parties, something few consumers would voluntarily assent to.[122]

Key elements of a unified cybersecurity and privacy framework should include:

- Strong privacy protections modeled on those contained in the European Union's General data Protection Regulation (GDPR). These rules give individuals control over their personal data, prohibiting the excessive compilation of data without individual's affirmative consent, establishing remedies for violations, setting a process to curb unfair practices and providing businesses regulatory certainty and a level playing field.[123]
- Mandated built-in security for online products and connected devices.
- Rules that impose duties on manufacturers and service providers to proactively prevent data breaches, make timely reports of breaches to consumers and law enforcement authorities, and, at a minimum, hold them liable for failing to comply with established standards.[124]
- Guarantees that states may require and enforce their own heightened cybersecurity and data protection standards.[125]

This final point – that federal rules should not preempt stronger state standards – is absolutely essential. The business desire for uniformity and harmonization must not run roughshod over the rights of states to maintain and enforce stronger standards. In this particular area, states have been far more protective of consumer and privacy interests than the federal government, and there is every reason to expect them to remain more nimble and responsive to consumer imperatives in the years ahead.

---

[122] Kimberly Kindy, "How Congress Dismantled Federal Internet Privacy Rules," Washington Post, May 30, 2017, available at: https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?noredirect=on&utm_term=.4254a345f6c7.

[123] European Commission, 2018 Reform of EU Data Protection Rules, available at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[124] See, for example, Rep. Cicilline's Consumer Privacy Protection Act, H.R.4081 (and companion introduced by Senator Leahy, S. 2124).

[125] See Laura Moy, hearing on "Protecting Consumers: Financial Data Security in the Age of Computer Hackers," House Financial Services Committee, May 14, 2015, available at: https://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-lmoy-20150514.pdf and Edmund Mierzwinski, hearing on "Data Security: Vulnerabilities and Opportunities for Improvement," House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit, November 1, 2017, available at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-emierzwinski-20171101.pdf.

B. Financial Regulation

As argued above, inadequate financial regulation and regulatory enforcement led directly to the Great Recession and its massive damaging impact on America. Recent, ongoing and pervasive financial sector abuses, including but definitely not limited to Wells Fargo and Equifax, conclusively demonstrate the need for tougher, not weaker, regulatory standards.

Wall Street continues to complain about excessive regulation and, occasionally, about regulatory duplication. The division of federal responsibility for prudential regulation of financial institutions certainly leads to some regulatory fragmentation, which has resisted reform, including during consideration and passage of the Dodd-Frank Act. Historically, and until creation of the Consumer Financial Protection Bureau, the worst consequence of that fragmentation was the failure to protect consumer interests. Secondary impacts, perhaps now modified by Dodd-Frank reforms, were regulator failure to adequately protect against systemic risks and extreme events, and problems – such as the AIG credit default swaps – falling through the cracks. It is unclear how consequential the current fragmentation is. What is clear is that some calls for eliminating duplication are disguised efforts to eliminate agencies and regulations opposed by Wall Street that advance important public interests (e.g., the call to fold the Office of Financial Research, currently an independent office to support the Financial Stability Oversight Council, into the Department of Treasury).[126]

But the most important point about financial regulatory complexity is this: That complexity is necessitated by the complexity of the financial corporations and financial markets. It absolutely would be ideal to lessen regulatory complexity, especially prudential regulation and measures designed to reduce systemic risk. The only responsible way to achieve this objective is to reduce the complexity of financial corporations, which means to adopt simple rules to split them up into smaller businesses with narrower focuses. The 21st Century Glass Steagall Act is an exemplar of how to achieve that objective; Public Citizen proposed a fuller agenda to achieve this objective in *Too Big: The Mega-banks are Too Big to Fail, Too Big to Jail, and Too Big to Manage*.[127]

C. Health Care Regulation

Like the financial industry, health care companies have also complained about "regulatory overload," notably in an October 2017 report from the American Hospital Association (AHA).[128] The AHA study purports to show administrative compliance costs of $39 billion annually, for 629 discrete regulatory requirements pertinent to hospitals and post-acute care providers, and claims that "many requirements are redundant, contradictory and provide little or no value."

Yet as is typical with such complaints, the evidence of regulatory duplication is minimal, the basis for purported regulatory cost claims is murky at best, and benefits are completely ignored.

---

[126] See Department of Treasury, A Financial System that Creates Economic Opportunities, June 2017, available at: https://www.treasury.gov/press-center/press-releases/Documents/A%20Financial%20System.pdf.

[127] Bartlett Collins Naylor, *Too Big: The Mega-banks are Too Big to Fail, Too Big to Jail, and Too Big to Manage*, Public Citizen, 2016, available at: https://www.citizen.org/sites/default/files/toobig.pdf.

[128] American Hospital Association, Regulatory Overload: Assessing the Regulatory Burden on Health Systems, Hospitals and Post-Acute Care Providers, October 2017, available at: https://www.aha.org/system/files/2018-02/regulatory-overload-report.pdf.

These brief comments can be made about the AHA study, which of course was conducted by an industry trade association with a self-interest in inflating cost estimates:

- The report completely fails to document the benefits of the regulatory standards it analyzes. These are acknowledged, but no monetary or health accounting is done of their benefits. (More on this point below.)
- The study methodology cannot be adequately assessed given the lack of details about the limited "convenience" sample of hospitals surveyed and how the survey was conducted and framed. There is no discussion of how the survey was developed and validated before being implemented, nor a clear discussion of how cost estimates were derived by surveyed institutions.
- Although the report claims to identify rules to eliminate that will not diminish patient outcomes, it does not analyze or explain how its reforms will safeguard patient interests.
- Similarly, the report does not identify the redundant requirements that it claims are commonplace and which should be eliminated. For example, it complains about 80 Centers for Medicare and Medicaid Services quality measures, but does not provide examples of how these well-vetted measures are "duplicative and misaligned."
- It correctly complains about the huge administrative costs associated with the American health care system, but fails to note that this cost is due primarily to the role of multiple, private payers. Indeed, it is notable that the AHA focuses on regulation while avoiding the extraordinary amount of time and resources allocated to billing.
- Many of the report's recommendations do not appear to stem from the underlying study.

None of this is to say that current health care regulations get everything right or provide all the right incentives. They plainly do not. But they are intended to address profound flaws in health care delivery and widespread fraud – problems of the private sector that demand regulation.

Health care quality in the United States is dramatically below standards in other rich nations, ranking last or nearly last in almost every key metric: care process, access, administrative efficiency, equity and health are outcomes. We have the highest rate of mortality amenable to health care; the second highest patient reported rate of medical, medication and lab mistakes; and the worst infant mortality rates.[129]

Medical malpractice is a nationwide scourge, with the best estimates now conservatively suggesting that malpractice kills 250,000 patients a year, making it the third highest cause of death in the nation.[130] A pre-Affordable Care Act HHS Inspector General survey found that almost one-in-six Medicare beneficiaries experienced an adverse event during their hospital stay.[131] The New York Times reports that, since 2013, 40 percent of the nation's nursing homes

[129] Eric C. Schneider, et. al., Mirror, Mirror 2017: International Comparison Reflects Flaws and Opportunities for Better U.S. Health Care, Commonwealth Fund, July 2017, available at: https://www.commonwealthfund.org/sites/default/files/documents/___media_files_publications_fund_report_2017_jul_schneider_mirror_mirror_2017.pdf.

[130] Martin Makary and Michael Daniel, Medical Error – the Third Leading Cause of Death in the US, May 3, 2016, *BMJ 2016; 353* available at: https://doi.org/10.1136/bmj.i2139.

[131] Daniel Levinson, Inspector General, Department of Health and Human Services, Adverse Events in Hospitals: National Incidence Among Medicare Beneficiaries, November 2010, available at: https://oig.hhs.gov/oei/reports/oei-06-09-00090.pdf.

have been cited for a serious violation, resulting in fines two-thirds of the time (the Trump administration is radically diminishing the use of penalties for such violations).[132]

Along with profoundly troubling quality of care issues, our health care system is bedeviled by massive fraud. The FBI estimates the cost of health care fraud as between 3 and 10 percent of overall health care spending — $82 billion to as much as $272 billion annually.[133] Along with billing fraud, improper prescription drug marketing, sales and rebate schemes are commonplace.[134]

The extensive regulation in the health care sector is designed primarily to address these twin problems: low-quality care and widespread fraud. Existing regulation is obviously inadequate to address these issues, but the problems would be dramatically worse in the absence of the rules on the books.

V. Conclusion

While opportunities for better regulatory coordination, more rigorous regulatory frameworks, an improved rulemaking process and enhanced regulatory standards abound, the evidence of widespread and consequential problems with regulatory duplication is weak. Much of what is touted as duplication appears to be camouflaged complaints about regulation itself. Yet corporate concerns about costs of regulation frequently fail even to acknowledge the benefits of regulation. And the best evidence on the costs and benefits of regulation shows that benefits vastly exceed costs, even by corporate-friendly accounting metrics.

There should be a bipartisan pathway forward on regulatory reform, focusing on:

- Increased transparency, focusing especially on the operations and influence of the Office of Information and Regulatory Affairs;
- An expedited rulemaking process not subject to manipulation by corporate insiders;
- Strong limits on the revolving door problem at regulatory agencies – one of the worst manifestations of the rigged system that partisans on all sides denounce;
- Respect for states' rights to establish more protective standards for their citizens than required by the federal government;
- Affirmative legislative and regulatory action to address everyday concerns of all Americans, including issues such as online privacy, excessive drug prices and concentrated and poorly functioning markets in sectors such as telecommunications, as well as to address unfair treatment of small businesses by large corporations; and
- Stronger rules and more resources for robust regulatory enforcement, to ensure that large corporations as well as small businesses play by the rules.

---

[132] https://www.nytimes.com/2017/12/24/business/trump-administration-nursing-home-penalties.html

[133] Federal Bureau of Investigation, Financial Crimes Report to the Public, Fiscal Years 2010-2011, available at: https://www.fbi.gov/file-repository/stats-services-publications-financial-crimes-report-2010-2011-financial-crimes-report-2010-2011.pdf/view.

[134] See Sammy Almashat, et. al., Twenty-Seven years of Pharmaceutical Industry Criminal and Civil Penalties: 1991 Through 2017, Public Citizen, March 14, 2018, available at: https://www.citizen.org/sites/default/files/2408.pdf.

Thank you for the opportunity to testify today, and we look forward to working with the committee on a shared agenda for the American people.

Mr. PALMER. I thank the gentleman.

The chair now recognizes Mr. Feeney for his testimony.

STATEMENT OF CHRISTOPHER FEENEY

Mr. FEENEY. Chairman Palmer, Ranking Member Raskin, and members of the subcommittee, thank you for inviting me to testify today. My name is Chris Feeney. I'm the executive vice president of the Bank Policy Institute and president of our Technology Policy Division, BITS.

Cybersecurity is a top-of-mind issue for every one of our CEOs, and the industry has been and remains committed to making the investments necessary to protect our critical infrastructure broadly. We embrace the trust that our customers confer in us and take the job of protecting customers and their data seriously, including valuing their privacy.

Our industry is heavily regulated. In the U.S. alone, we have 9 independent Federal regulators, 3 self-regulatory organizations, and 50 State banking, securities, and insurance agencies. Regulations include extensive cybersecurity oversight and comprehensive data protection standards, such as those in the 1999 Gramm-Leach-Bliley Act.

The cybersecurity requirements across the industry are very diverse in terms of size, type of business, and geographic footprint. Yet we have validated that over 80 percent of the cyber issuances are common across all regulators.

For the financial sector, it becomes a tangible problem when those tasked with creating cybersecurity rules approach regulations with their own variations, addressing the same cyber requirements with different approaches and language.

To analogize this, think of the impact on your safety if air traffic controllers didn't use English as a common language and instead pilots were required to use their native language for every airspace they pass through. This would be challenging at best, require extensive training, and introduce unneeded risk.

This is the dilemma we face today with variations on cyber standards, requirements, and expectations without any appreciable benefit to security. These requirements lead to misuse of scarce cybersecurity experts' time, taking them away from protecting our technology and the customers who count on us daily to access ATMs, to write checks, and to pay mortgages.

When a chief information security officer at one of our largest firms estimates that 40 percent of their time is spent trying to unravel the web of cybersecurity regulation rather than focusing on protecting systems, that's a serious problem.

We face similar complexity in the area of data breach, which has no uniform standard, and we are seemingly entering into a complex environment of conflicting requirements related to privacy as regulation develops around international requirements, emerging State requirements, and potentially local requirements, such as those being discussed in Chicago.

For technology and cybersecurity experts, consistency, repeatability, and improved security require a common technical and operating architecture, a common language, and a common framework to achieve the highest degree of protection.

In a 2017 Financial Stability Board publication, U.S. member agencies self-reported that 10 different Federal schemes of cyber regulation were in place and that 43 different publicly available cybersecurity issuances were about to be offered.

We want to be clear. The financial industry supports the need for cyber regulation and the industry's multi-billion-dollar investments here to improve our capabilities and satisfy our regulations. These investments have contributed to developing the highest standards for cybersecurity, data security, and customer expectation.

Individually these regulations have merit. However, when one regulation is laid over another and another, it saps both the time and focus from executive leadership and those whose time and job it is to defend and operate our businesses. And more specifically, firms are already burdened by a shortfall of skilled cyber professionals and they must take resources away from protecting their platforms to interpret the language of divergent regulation.

Ultimately, we hold ourselves accountable for protecting customers, our systems, and for compliance with the regulatory process. You might be surprised to hear me say that the solution is not fewer regulations but instead rationalized and harmonized regulation around a common approach and a shared language.

BITS and our industry partners have developed a model cyber framework. The foundation of this effort centers on the NIST Cybersecurity Framework which is used across multiple industries, Federal and State government, and with support from both the Obama and the Trump administration.

The financial sector used this standard to develop a sector profile. And importantly, we developed a solution by working with our regulators, gathering their input, incorporating their diagnostic statements, and tailoring the solution so that we don't force a one-size-fits-all approach to managing cyber risk.

There are clear benefits of this approach for the regulatory agencies, such as examinations that can be tailored to institutional complexity, and for financial firms, such as optimizing the use of cybersecurity professionals' time and also enabling more effective use of fintech innovators who can meet requirements and expectations more efficiently.

Congress has been vocal in encouraging regulators to pause any additional cyber regulation, and we ask that Congress now support and encourage the use of the sector profile.

In the spirit of this committee's broad remit, we also ask that Congress work to develop uniform Federal standards for data breach notification and a common privacy standard before we enter into a 50–State and 50-variation environment similar to what we face today in cyber. We must ensure these issues do not fall prey to jurisdictional battles, and we need to work together to maintain the cyber integrity of the U.S. financial system.

Thank you, Mr. Chairman, and I look forward to your questions.

[Prepared statement of Mr. Feeney follows:]

Testimony of

Christopher F. Feeney

On behalf of

BITS – Bank Policy Institute

Before the

House Subcommittee on Intergovernmental Affairs

for the

Committee on Oversight and Government Reform

Hearing entitled:

"Regulatory Divergence: Failure of the Administrative State"

July 18, 2018

Chairman Palmer, Ranking Member Raskin, and members of the Subcommittee, thank you for the opportunity to testify before you today.

My name is Christopher F. Feeney, and I am the President of BITS – Business-Innovation-Technology-Security.[1] BITS is the technology policy division of the Bank Policy Institute (BPI). BITS provides an executive level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector.

Led by C-Suite executives, including Chief Executive Officers (CEOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and other senior leaders, BITS brings together its members, regulators, government agencies and technology firms to advance collaboration in the regulatory and risk environment; address current and emerging policy issues; improve effectiveness of technology programs; promote critical infrastructure resilience; and strengthen cybersecurity and reduce fraud.

With a focus on business, innovation, technology and security, BITS is a leading voice in Washington for information sharing and development of best practices and policies that protect our nation's financial services platforms and the customers they support.

In addition to my role as BITS President, I am also a member of the Financial Services Sector Coordinating Council's (FSSCC) Executive Committee and Co-chair of the Policy Committee. The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U.S. Federal government, and coordinating crisis response for the benefit of the Financial Services sector, consumers and the nation.[2] I also hold leadership positions in several other industry organizations, such as Sheltered Harbor and fTLD Registry Services, LLC, all of which are focused on addressing the security and resiliency of financial institutions.

In these roles, my charge is to advance policies to protect the nation's financial infrastructure, firms' infrastructure and, most importantly, to protect the customers that use and depend on these financial systems every day. On behalf of our member firms, I offer the following testimony regarding the growing challenges financial firms face, putting a particular emphasis on a multi-year process the financial sector undertook to make progress relative to harmonizing cybersecurity regulation in the U.S. and globally. The key areas to cover are:

1) The expanding number of cybersecurity issuances financial firms are being asked to adhere to and the solution industry is proposing for usage by the regulatory community;

---

[1] For more information, please visit: https://www.bpi.com and https://bpi.com/category/bits/.
[2] For more information, please visit: https://www.fsscc.org/

2) The fast-changing environment to address the issue of privacy as evidenced by recent state and international privacy laws; and

3) The ongoing need for a uniform federal standard for data protection and breach notification.

A. Introduction

Financial firms prioritize preserving customer trust, and make significant investments to protect and secure customers' personal and financial information. As an industry, financial services is one of the most advanced when it comes to cybersecurity protections and regulators regularly oversee and challenge the systems and processes firms have in place to protect information and privacy. The industry is subject to multiple laws – for example, the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act – that include strong cybersecurity requirements, consumer protections and govern the industry's use of data.

On an individual basis, many of the regulatory requirements financial firms must meet are beneficial and have strengthened firms and the industry. The challenge is that collectively, without harmonization and alignment, the regulations are often counterproductive; creating duplication, conflict and confusion, and place a significant burden on firms' ability to improve cybersecurity and innovate to stay ahead of threats.

Cybersecurity regulation is a ready example. Several years ago, as regulators (see Figure 1) began issuing multiple new cybersecurity tools, guidance and requirements, firms became deeply concerned that they were having to divert cybersecurity resources away from the front lines of cyber protection to instead focus on regulatory compliance – an outcome that put firms at risk and most certainly did not meet regulators' intentions of helping protect the industry against threats.

Over the course of the last three years, BITS has worked to address this problem and has coordinated extensively with firms, industry associations, our industry's sector coordinating council, the U.S. Department of the Treasury, our regulators and other federal agencies to develop a path forward that meets regulators' expectations while giving firms the ability to increase focus on improving front line cyber defenses rather than regulatory compliance. The solution we have developed – referred to as the Sector Profile – is described below. We are currently working to have the Sector Profile, which is based on the commonly used and cross sectoral National Institute of Standards and Technology's (NIST) Cybersecurity Framework, adopted across multiple jurisdictions and internationally.

Another example – and the most recent – is in the data privacy arena. While existing law and regulation for financial firms includes privacy and data security measures, the European Union's General Data Protection Regulation (GDPR) as well as the California Consumer Privacy Act (CCPA) create new obligations for firms that will require changes to

technology, policies and procedures. While both laws may create an entirely new set of requirements to enable consumers to control how their data is used across all industries, they also set up a number of duplicative requirements and potential conflicts with existing regulations for financial firms.

For instance, financial firms must fulfill what are referred to as Know-Your-Customer (KYC) requirements to detect and prevent money laundering. To fulfill these obligations, firms must collect and retain certain personal and financial information on customers for a defined period of time (e.g., in the securities area FINRA Rule 17a-4 requires customer record retention for 7 years). Under GDPR and CCPA, a consumer can request that their information be deleted, setting up a potential conflict for firms who must now meet competing and mutually exclusive requests.

A growing concern for financial firms is that GDPR and CCPA may be the start of a new wave of similar but different privacy laws being considered across the country by states as well as cities and warrants consideration of a national standard. If the history of state data breach laws is any indicator, firms may soon face 50 different standards they must comply with and, in some cases, de-conflict with multiple government authorities.

Lastly, the financial industry has been a strong proponent of a single, national data protection and breach notification standard to help firms and consumers protect themselves and recover in the event of a breach. We have testified in support of such legislation, most recently before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit on its "discussion draft" entitled, "Data Acquisition and Technology Accountability and Security Act," calling for a uniform, federal consumer data protection and breach notification law.

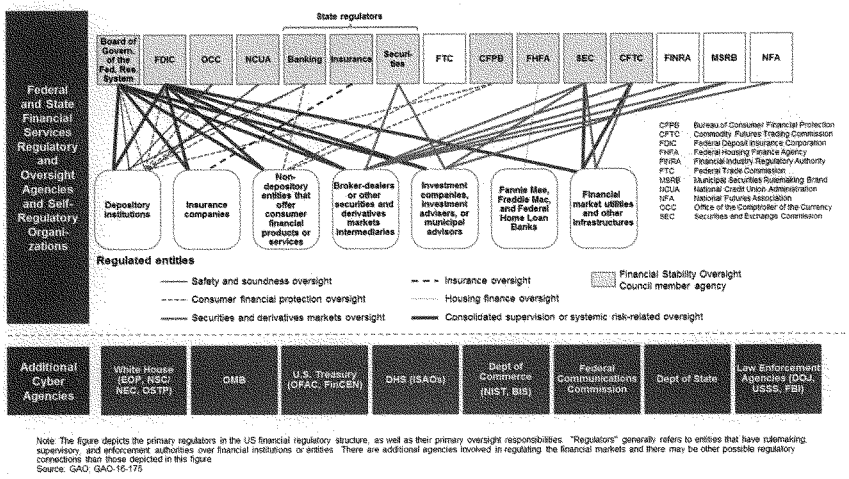
This Committee's support for the regulatory harmonization effort would be welcomed and we encourage you to help ensure competing frameworks and requirements for other aspects of data security, breach notification and privacy can be better aligned under a national standard.

B. Overview and Challenges Inherent in the Financial Services Sector Regulatory Structure

The financial services sector consists of more than 13,000 banks and credit unions, payment companies, insurance companies, wealth and asset managers and financial market utilities that process transactions, payments and move money across domestic and international markets.

The sector is overseen by nine federal regulators (all of which are independent from the executive branch), three self-regulatory organizations, the U.S. Department of the

Treasury (Treasury) as its sector-specific agency,[3] and every state banking, insurance, and securities agency. When agencies tasked with cybersecurity-related authorities are added, the list expands even further (see Figure 1).



Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure.
Source: GAO. GAO-16-175

(Figure 1. The current financial services regulatory structure as it relates to cybersecurity)[4]

C. The Financial Services Sector's Commitment to Cybersecurity Advancement

Cybersecurity is a top priority for our member firms. It is a key concern and focus area for CEOs and Boards of Directors, all the way to the frontline defenders sitting at keyboards monitoring network activity and responding to security events. Firms' senior management have made clear that cybersecurity risk is not solely a technology issue, but a business line and enterprise-wide risk that should be considered across all levels of the organization. As such, cybersecurity is a regular agenda item at Board of Directors meetings, often with the Chief

---

[3] For more information, please visit: https://www.dhs.gov/financial-services-sector

[4] Figure is derived from a nearly identical graphic developed and used by the United States Government Accountability Office in its February 2016 report, entitled, "Financial Regulation: Complex and Fragmented Structure Could be Streamlined to Improve Effectiveness," which was then amended to include the agencies below the dotted line. See: https://www.gao.gov/assets/680/675400.pdf. Those agencies were added because their cybersecurity issuances also can have a direct impact on financial institutions' cybersecurity programs and compliance response.

This exact graphic, however, has been reproduced from the FSSCC and BCG Platinion May 17, 2017 presentation at the NIST Cybersecurity Workshop event:
https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf

Information Security Officer or equivalent providing updates on threats to the financial industry and individual firms, specific risks plus risk trends, and strategies for mitigation. With this senior-level support, firms have sharpened priorities and their commitment to cybersecurity.

According to the Cyber Security Market Report "U.S. Financial Services: U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020" report, the U.S. financial sector's cybersecurity market is the largest and fastest growing private sector cyber security market. Its cumulative 2016-2020 market size is forecasted to exceed $68 Billion.[5]

Recognizing that cybersecurity affects the entire industry, financial firms also have a long history of significant investment and collaboration to improve cybersecurity preparedness, response and resiliency across the sector. For example, prior to the passage of the Homeland Security Act of 2002 and the Cybersecurity Act of 2015, the financial services sector established the cyber threat information sharing and analysis center known as the FS-ISAC – a gold standard for critical infrastructure cyber threat information sharing organizations.

In addition, BITS has facilitated ten semi-annual CEO-led "Joint Financial Associations Cybersecurity Summits." These summits bring together financial institution CEOs, trade association CEOs, and key Congressional and government leaders to actively address sector resiliency, respond to capability gaps, and encourage coordination and investment. Other sector-wide activities include the initiation of a joint financial services, telecommunications, and electric sector working group to address cyber risks posed to all three sectors; the "Hamilton Series" of cybersecurity response exercises; the establishment of a not-for-profit organization – Sheltered Harbor – an initiative launched by the financial services industry to establish standards for secure data vaulting and rapid recovery of customer balances and assets in the event of a catastrophic cyber incident; fTLD Registry Services, secure website domains for banking and insurance companies; and updates and testing of the sector's cyber response plans, including the "All-Hazards Crisis Response Playbook," which provides guidance on intra-sector and government coordination in the event of a cyber incident.

Much of this collaborative work includes regulators, and our government partners at the Treasury and Department of Homeland Security (DHS). Under the DHS National Infrastructure Protection Plan, Treasury is our sector-specific agency and helps organize regular meetings of the FSSCC along with our government counterparts, referred to as the Financial and Banking Information Infrastructure Committee (FBIIC). These meetings help our industry, our regulators and our government partners work collaboratively to improve resiliency and the policies that enable it.

[5] https://homelandsecurityresearch.com/reports/u-s-financial-services-cyber-security-market/

D. The Issue of Cybersecurity Regulatory Overlap

Industry and our regulators share the same goal: To ensure the financial services sector is safe, sound, strong and secure. We support our regulators' attention to the critical issue of cybersecurity and understand that on a daily basis the nation's businesses and citizens rely on our ability to facilitate the financial transactions of their daily lives. We also understand and embrace the fact that we are the guardians of our customer's data, including sensitive personal and financial information. Accordingly, like the regulatory community that oversees us, we support the advancement of cybersecurity and data protection and understand the need for their regulatory oversight.

With a fragmented regulatory landscape, however, we are now experiencing a proliferation of layered requirements that often are topically similar, but semantically different. Some of these cybersecurity proposals incorporate the NIST Cybersecurity Framework's organizational structure and terminology (a congressionally approved framework supported by both the Obama and Trump Administrations). But many do not, instead opting for novel approaches and different language. For those financial institutions operating internationally, or even servicing international customers within the United States, the number of applicable regulatory schemes only expands.

United States Financial Services Cybersecurity Regulations, Guidance and Supervisory Practices: In 2017, the Financial Stability Board[6] published its "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices"[7]. U.S. member agencies self-reported 10 different federal "schemes" of regulation that "address cybersecurity" for the financial services sector and cited 43 different publicly available cybersecurity issuances. The 10 schemes and 43 issuances did not include agency/examiner questionnaires, first-day letters, and other non-public supervisory expectations that financial institutions are also subject to during their examination process, nor does it include the cyber regulatory expectations issued or proposed by each of the fifty states.[8]

---

[6] The Financial Stability Board (FSB) is an international body that monitors and makes recommendations about the global financial system. The FSB, working through its members, seeks to strengthen financial systems and increase the stability of international financial markets. The policies developed in the pursuit of this agenda are implemented by jurisdictions and national authorities.

Members include representatives from financial services regulatory oversight bodies from the following 25 jurisdictions: Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States and the European Union.

For more information, please visit: www.fsb.org.

[7] See: http://www.fsb.org/wp-content/uploads/P131017-2.pdf

[8] In my written testimony before the Senate Homeland Security and Governmental Affairs Committee last year, I supplied charts of the over 30+ issuances that we had been tracking since the release of the NIST Cybersecurity Framework in 2014 that directly impacted firms in the financial services sector. Those charts can be found in

Select International Cybersecurity Regulations, Guidance and Supervisory Practices: The international financial services regulatory community has also been prolific. Indeed, each of the 25 member jurisdictions to the FSB reported that "they have publicly released regulations or guidance that address cybersecurity for at least part of the financial sector, and a majority have also publicly released supervisory practices."

Like the United States, the European Union (EU) self-reported 10 schemes of regulation that pertain to the financial services sector. Additionally, the EU cited to 26 applicable and publicly available cybersecurity issuances. Each overlapping FSB and EU member nation reported that they also had their own nation specific regulatory schemes.

In the Asia-Pacific region, Japan reported 4 publicly available supervisory documents, China 11, and Australia 11 as well.

Future Cybersecurity Regulatory Issuances: According to the Stocktake, 72% of the member jurisdictions self-reported that they also intend to issue more cybersecurity expectations in the near future. Items listed, included: new regulations, "guidance and strategy for the financial sector; a self-assessment exercise to gauge the cyber resilience of FMIs; guidance on conducting threat intelligence based testing of cyber resilience; developing a set of standards for industry on Information Technology Risk (including cyber) and updating existing guidance in this area; and establishment of a computer emergency response team (together with computer security incident response team referred to hereinafter as CERT) for the financial sector."

E. The Impact of Cybersecurity Regulatory Overlap

The current fragmented approach to cybersecurity regulation causes firms to expend substantial personnel and resources reconciling notionally similar, but semantically different cybersecurity proposals and agency expectations. More specifically, it introduces inefficiencies by requiring institutions to identify, draft, and compile functionally equivalent sets of data from and for the same systems to satisfy each different regulator and each different regulatory standard. As a result, institutions are forced to create single-use compliance data, rather than focusing their time on developing security and mitigation techniques that improve a firm's cybersecurity program and protects customers.

When the sector surveyed its information security teams approximately two years ago, one firm estimated that 40% of its cyber team's time was spent on compliance related

---

Appendix A and can be accessed here: https://www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf.

Since that time, we have not resumed the tracking because of the volume of proposals at the State and International level.

matters, not on cybersecurity. That multinational's experience was not unique. Due to one framework issuance, in particular, the reconciliation process delayed another firm's implementation of a security event monitoring tool intended to better detect and respond to cyber-attacks by 3-6 months.

While each agency proposal or set of requirements may have its own merit, when continuously layered, the added complexity is unsustainable as there are simply not enough cybersecurity professionals available to perform the necessary work. According to the 2017 jointly issued Cybersecurity Ventures – Herjavec Group report, there were an estimated 350,000 unfilled cybersecurity jobs in the United States for 2017. This trend is only expected to continue, with the global shortfall reaching 2 million by next year, and by as much as 3.5 million by 2021.

The lack of harmonization also complicates efforts to coordinate across critical infrastructure sectors and with the federal government for cyber incident response. A key focus for the federal government and DHS, in particular, has been to foster a "whole of nation" approach to cybersecurity. This effort to foster greater public-private partnership is critical if we are to effectively protect our economy, our customers, and our citizens from cyber threats. As regulations pull financial institutions away from using the more recognized and widely deployed NIST-based approaches, this could endanger not only our sector, but other critical infrastructure sectors if a coordinated response is needed.

F. A Proposed Cybersecurity Solution and the Regulatory Community's Response to Date

There is a solution, however: the Sector Profile, a meta-framework for financial services based on the organizational structures of the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (NIST Framework)

The industry first suggested regulators align their efforts more closely to the NIST Cybersecurity Framework in a September 21, 2015 submission[9] to the Federal Financial Institutions Examination Council, a coordinative body for the banking-specific agencies and organizations[10]. This suggestion included a request that regulators work collaboratively with

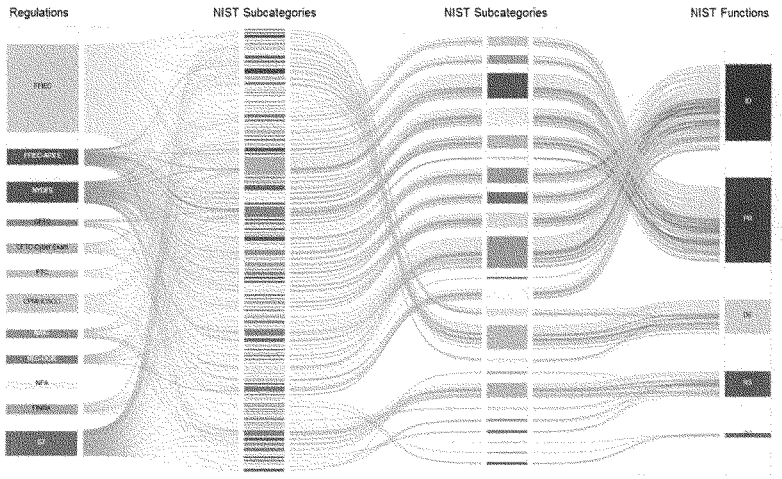
[9] See: https://www.fsscc.org/files/galleries/FSSCC_FFIEC_Cybersecurity_Assessment_Comment_Letter_(FR_2015-17907).pdf

[10] For more information on the FFIEC, including its membership and statutory authorities, please see: https://www.ffiec.gov/. Chaired by the U.S. Department of Treasury's Assistant Secretary for Financial Institutions, members include representatives from the 2) American Council of State Savings Supervisors, 3) Commodity Futures Trading Commission, 4) Conference of State Bank Supervisors, 5) Consumer Financial Protection Bureau, 6) Farm Credit Administration, 7) Federal Deposit Insurance Corporation, 8) Federal Housing Finance Agency, 9) Federal Reserve Bank of Chicago, 10) Federal Reserve Bank of New York, 11) Federal Reserve Board, 12) National Association of Insurance Commissioners, 13) National Association of State Credit Union Supervisors, 14) National Credit Union Administration, 15) North American Securities Administrators Association,

industry to find a solution that would allow regulators to fulfill their responsibilities while better allowing firms to focus on critical cybersecurity activities.

In October 2016, industry (through the FSSCC) and our government coordinating council, the FBIIC, agreed to a joint working group to discuss opportunities to better harmonize cybersecurity related requirements and expectations. When it became clear that the FBIIC would be unable to meet on an ongoing basis, the sector moved ahead on its own with regular individualized outreach to the various regulatory agencies, all of which expressed some level of support for the industry initiative.

To start, the sector began mapping multiple cybersecurity related issuances and proposals against both the NIST Framework and importantly standards from the International Standards Organization (ISO). With the initial mappings complete, a clear pattern emerged: Over 80% of the mappings were topically identical, but semantically different. (See Figure 2. below).



(Figure 2. Regulatory Overlap and Complexity in Reconciling Select Proposals to the NIST CSF).

To reduce the time cybersecurity personnel allotted to reconciling semantic differences, the industry then chose to fund an effort to use these mappings to develop the Sector Profile. Based on the mappings and the widely accepted use of the NIST Framework, the Sector Profile was architected around the NIST Framework's five functions, categories, and

16) Office of the Comptroller of the Currency, 17) Securities and Exchange Commission, and 18) Securities Investor Protection Corporation.

subcategories, and extended to include two new functions – Governance and Supply/Dependency Management – which emerged as distinct areas of (appropriate) regulatory focus. The architecture also extended the NIST-based structure so that it could function as a compliance assessment tool. Borrowing from the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool's "Declarative Statements," the Profile added a series of Diagnostic Statements, which synthesize overlapping expectations from multiple regulatory organizations into a more singular, standardized set of assessment-ready diagnostics.

Because of its NIST basis, NIST asked the sector to preview that work at it NIST Cybersecurity Framework Workshop in May 2017. In the months that followed, the sector met individually with each of its federal regulatory agencies, the various self-regulatory organizations, and associations for state-based regulators. The feedback collectively was that it was a productive body of work and that we should continue to refine it, adding risk tiers so that it would be usable and applicable to the most sophisticated firms and the least sophisticated firms. In April 2018, NIST sponsored a one-day, open-to-the-public event at the Department of Commerce specific to the latest round of tailoring work. Again, the Sector Profile was seemingly well-received by all in attendance, including representatives from the various regulatory agencies.

G. Benefits to Regulators, Financial Firms and the Financial Infrastructure

As of today, the tailoring work continues, and is near complete. The sector anticipates releasing a fully developed Sector Profile "Version 1.0" around September. While the agencies have voiced support for its development, we will also be seeking acceptance for its usage. If used by the regulators, the benefits to the regulators, the financial services sector, and those citizens and customers that depend on the financial system would be manifold.

With its usage, the regulatory community will be able to:

- Tailor examinations to institutional complexity and conduct "deeper dives" in those areas of greater importance to that particular regulatory agency;
- Better discern the sector's systemic risk, affording more agency time for specialization, testing and validation;
- Create the ability to take collective action to better address identified risks;
- Compare and better analyze data from other agencies and other jurisdictions;
- Enhance regulators visibility into non-sector and third party risks.

For financial institutions, the benefits are likewise numerous:

- Optimization of cybersecurity professionals' time "at the keyboard" and defending against current and next generation attacks (e.g., calibrating risk identification, automating controls, cyber range testing, instrumenting monitoring systems,);

- Improved Boardroom and Executive engagement, understanding and prioritization;
- Enhanced internal and external oversight and due diligence;
- Greater innovation as technology companies, FinTech firms, startups, etc., are able to meet requirements expectations more efficiently;
- More efficient third-party vendor management review and oversight; and
- Greater intra-sector, cross-sector and international cybersecurity collaboration and understanding.

H. Conclusion and Congressional Request

Congress has an important role to play in –

(1) publicly supporting cyber regulatory harmonization and cyber regulation consistency by encouraging regulators to use and adopt the Sector Profile;
(2) in offsetting the potential proliferation of state and local privacy laws and enhancing consumers' rights to privacy before a patchwork of inconsistent and potentially incongruous privacy requirements are developed; and
(3) in legislating uniform standards for data breach reporting by developing clear, concise and effective notification standards.

With respect to cybersecurity, the financial services sector shares the same goals with the regulatory community: advancing the safety, soundness, and resilience of the financial system by protecting financial institutions and the financial sector from increasing cybersecurity risks. Given the complexity of our regulatory environment, a lack of harmonization negatively impacts the ability of financial institutions to devote resources to security activities, and this is exacerbated by the shortage of cybersecurity professionals. We hope all would agree that those professionals that are available should be able to devote more time to security rather than interpreting notionally similar, but semantically different regulatory expectations.

As discussed, the Sector Profile, if supported, will provide a mechanism for alignment to current regulatory expectations, requirements, and authorities. Additionally, and perhaps more importantly, the Profile provides a clear path forward to streamline existing and future cybersecurity regulatory expectations around a common structure and vocabulary. Accordingly, we request that Congress continue to encourage regulators in their harmonization efforts and suggest public support and future alignment with the Sector Profile.

The same holds true for providing consumers and businesses with a clear expectation for how their data and privacy will be protected and what level of information, transparency and timing for notification they should expect if ever their information is improperly accessed and would result in risk of harm. Multiple standards with slightly different timeframes, definitions or other specific requirements will not benefit consumers and requires firms to sift through a myriad of different notification requirements when they would be better served

helping their businesses better protect information and privacy and attending to customers should a breach occur.

Lastly, the implementation of GDPR and the passing of the California Privacy Legislation both have the same objective to protect the privacy of individuals while offering choices for how individuals want to manage their personal information. The financial industry supports privacy advances and has been a strong advocate for protecting customer information for decades. We can forecast, however, that a proliferation of multiple privacy standards with multiple, and in certain cases conflicting criteria relative to existing laws, can lead to a negative outcome. As noted above, current law has provisions for handling sensitive customer information while also requiring retention of client information for seven years. These provisions are inconsistent with requirements in some of the new privacy issuances and puts a firm in the midst of a jurisdictional dilemma while a firms' interest is to ensure the protection of their customer. Working on a common federal standard for privacy protection that can complement existing requirements is a chance to get ahead of more disparate laws. We would ask Congress to develop a uniform privacy standard that the financial services industry and other industries who hold sensitive customer information could adopt and adhere to in a collective way.

In short, we stand ready to work with Congress on data breach and privacy standards and we will continue to work actively with our regulatory community on this more rationalized approach to cybersecurity regulation. As we do so, Congressional encouragement is welcome. Indeed, it is needed.

Mr. PALMER. I thank the gentleman.

The chair now recognizes Mr. Sherouse.

STATEMENT OF OLIVER SHEROUSE

Mr. SHEROUSE. Chairman Palmer, Ranking Member Raskin, and members of the subcommittee, thank you for the chance to speak to you today about the important and often overlooked problem of duplicative regulations and regulatory standards.

My testimony today will focus on one cause of regulatory duplication, the incomprehensible scale of the administrative state. And I will also present two ways my colleagues and I are working to reduce that problem. First, through the application of text analysis and machine learning in our QuantGov project; and second by developing an open, machine-readable, and data-first standard for rulemaking documents called XRRL.

Now, my job is policy analytics, and what that means is that I teach computers to read policy documents, and especially regulation. We have to use computers because the administrative state has grown to an incomprehensible size. And I mean that literally. There are simply too many rules for any one person to understand.

So using text analysis and machine learning, my colleagues and I have created a dataset called RegData to quantify Federal regulation.

Now, RegData tells us that today there are more than 103 million words in the Code of Federal Regulations, including 1.08 million individual regulatory restrictions, so that's words and phrases like "shall" and "must" that indicate a particular mandated or prohibited activity.

That means that if you were to read the Code as your full-time job, it would take you 3 years, 111 days, and a bit past lunchtime the next day. By the time you'd finished, of course, you would need to immediately start figuring out what had changed since you started. And that's no easy task since the Code increases by an average of more than 1.4 million words every year.

So since reading the Code is impossible, data tools like those we have produced for the QuantGov project can help us begin to make better sense of the administrative state. RegData, in fact, does more than count total words and restrictions. It attributes them to the individual agencies that write them and predicts which industries will be affected by them.

All of our data is freely available, and our website features a daily updated interactive tracker of Federal regulation which users can break down by industry and by agency.

And we do the same thing for regulation currently being developed with our RegPulse dataset, which examines rules as they are published in the Federal Register. And as with RegData, we have built a daily updated interactive tool that allows users to see which industries have more or fewer relevant rules coming into effect over the next several years and what those rules are.

With QauntGov we are producing these kinds of data and interactive tools for a growing set of jurisdictions and policy documents. The software we used to produce QuantGov is also open source and freely available for anyone to use or build on.

For a more comprehensive understanding of the administrative state, however, we should reexamine the medium by which regulations are made. The current process is made for paper, paper rules and analyses published in a paper Federal Register and compiled into a paper Code of Federal regulations.

Even the electronic versions of these documents essentially mimic the paper-based system in use since the Administrative Procedure Act of 1946. Seventy years later, it is time for an upgrade to an open, machine-readable, and data-first standard format for regulatory documents.

A standard format could liberate the information that's currently trapped in pretty dense prose about who regulations will affect and how and transform that information into accessible data.

That data can be used by Congress to ensure effective oversight. It can be used by regulators to avoid duplication across agencies and potentially even across jurisdictions. It could facilitate the review of regulatory programs to fix those that are broken and to recognize those that are successful. And it can be used by businesses and individuals to ensure that they know what the law is and how to follow it.

My colleagues and I are currently developing such a standard, the eXtensible Regulatory Reporting Language, or XRRL. Our role with this project is to build an open and nonproprietary standard incorporating insights from the academy, government, and industry that can be adapted to any level of government, including the U.S. Federal Government.

So in conclusion, duplication in regulation is a side effect of an administrative state grown too large to manage effectively, and tools like the ones we have built with QuantGov are a step towards making an incomprehensible collection of rules somewhat less so. But the implementation of an open, data-first standard format, such as XRRL for rulemaking, would be an even more powerful way to render the administrative state more manageable while also providing benefits to both those writing rules and those subject to them.

I thank you again for the opportunity to testify, and I look forward to answering your questions.

[Prepared statement of Mr. Sherouse follows:]

MERCATUS CENTER
George Mason University

TESTIMONY

REDUCING ADMINISTRATIVE INCOMPREHENSIBILITY WITH DATA TOOLS AND STANDARDIZATION

Oliver Sherouse
Policy Analytics Lead, Program for Economic Research on Regulation, Mercatus Center at George Mason University

House Committee on Oversight and Government Reform, Subcommittee on Intergovernmental Affairs
Regulatory Divergence: Failure of the Administrative State

July 18, 2018

Chairman Palmer, Ranking Member Raskin, and members of the Subcommittee on Intergovernmental Affairs:

Thank you for the chance to speak to you today about the important and often overlooked problem of duplicative regulations and regulatory standards. My name is Oliver Sherouse and I am the policy analytics lead for the Program for Economic Research on Regulation at the Mercatus Center, a 501(c)(3) academic research center at George Mason University.

My testimony today will focus on one cause of regulatory duplication: the incomprehensible scale of the administrative state. I will also present two ways my colleagues and I are working to reduce that problem: first, through the application of text analysis and machine learning in our QuantGov project; and second, by developing an open, machine-readable, and data-first standard rulemaking format called XRRL.

THE INCOMPREHENSIBILITY OF THE ADMINISTRATIVE STATE

Since "policy analytics" is not a very common phrase, I will explain what it is that I do more simply: I teach computers to read policy documents, especially regulation. We have to use computers because the administrative state has grown to an incomprehensible size. I mean that quite literally: there are simply too many rules for any one person to understand, whether that person is trying to follow those rules or write new ones. So using text analysis and machine learning, my colleagues and I have created a dataset called RegData to quantify how much regulation there is, who writes it, and whom it affects.

RegData tells us that today there are more than 103 million words in the *Code of Federal Regulations* (CFR), including 1.08 million individual regulatory restrictions—words and phrases such as *shall* and *must* that indicate a particular mandated or prohibited activity.[1] To put that number in context, if you were to read the CFR as your full-time job, at 250 words a minute for 40 hours a week, it would take you three years, 111 days, and a bit over 5 hours.

[1] Patrick A. McLaughlin and Oliver Sherouse, RegData US 3.0 Daily (dataset), QuantGov, Mercatus Center at George Mason University, 2018.

By the time you had finished, of course, you would need to immediately start figuring out what had been added in the interim. That's no easy task, since according to RegData, from 1970 to 2017 the CFR increased by an average of more than 1.4 million words and 14,000 regulatory restrictions every year.[2]

HOW QUANTGOV DATA TOOLS CAN HELP REDUCE INCOMPREHENSIBILITY

While reading, let alone understanding, the entire CFR is impossible, data tools like those we have produced for the QuantGov project at the Mercatus Center can help us begin to make better sense of the administrative state.

RegData, in fact, does more than count total words and restrictions. It attributes them to the individual agencies and departments that create those words and restrictions, and it predicts which industries will be affected by them. All of our data is freely available, and our website now features a daily updated interactive tracker with which users can break down federal regulation by industry and by agency.

We can use the same kind of text analysis to understand regulation currently being developed. To create our RegPulse dataset, our system examines rules as they are published in the *Federal Register* and, as with RegData, quantifies those rules, tracks the agencies promulgating them, and predicts which industries are likely to be affected by them. And as with RegData, we have built a daily updated interactive tool that allows users to see which industries have more or fewer relevant rules coming into effect over the next several years, and what those rules are.

With QuantGov we are producing not only these kinds of data, but also these kinds of interactive tools for states, for other countries, and for a broader spectrum of policy documents. The software we use to produce QuantGov is also open source and freely available for anyone to use, modify, and build on.

XRRL: RULEMAKING AS DATA

A more comprehensive understanding of the large mass of federal regulation, however, could be achieved by going one level deeper and reexamining the medium by which regulations are made. The current regulatory process is made for paper: paper rules and analyses published in a paper *Federal Register* and compiled into a paper *Code of Federal Regulations*. While there are now electronic versions of these documents, they essentially mimic the paper-based system in use since the Administrative Procedure Act of 1946.

Seventy years later, it is time for an upgrade. A modern approach to rulemaking should insist on the use of an open, machine-readable, and data-first standard format for regulatory documents. A standard format could liberate the information about whom regulations will affect and how they will be affected—information that is currently trapped in dense prose—and transform it into discoverable, machine-readable data.

That data can be used by Congress to ensure effective oversight. It can be used by regulators to avoid duplication within or across federal agencies and potentially even across jurisdictions. A modern regulatory standard could also facilitate the review of regulatory programs so that those that are broken can be fixed and those that are successful can be recognized. And it can be used by businesses to ensure that they know what the law is and what they need to do to follow it.

---

[2] Patrick A. McLaughlin and Oliver Sherouse, RegData US 3.1 Annual (dataset), QuantGov, Mercatus Center at George Mason University, 2018.

My colleagues and I are currently developing such a standard, the eXtensible Regulatory Reporting Language, or XRRL. Our goal with this project is to build an open and nonproprietary standard incorporating insights from the academy, government, and industry that can be adapted to any level of government.

CONCLUSION

Duplication in regulation is a side effect of an administrative state grown too large to manage effectively. Tools like the ones we have built with QuantGov are a step toward making an incomprehensible collection of rules somewhat less so, and we will continue to produce them. But the implementation of an open, data-first standard format such as XRRL for rulemaking would be an even more powerful way to render the administrative state more manageable, while also providing benefits to both those writing rules and those subject to them.

I thank you again for the opportunity to testify, and I look forward to answering your questions.

Sincerely,

Oliver Sherouse

Policy Analytics Lead, Program for Economic Research on Regulation
Mercatus Center at George Mason University

Mr. PALMER. I thank the gentleman for his testimony.

I think we'll go ahead and begin with our questions. We anticipate that they will call votes at any time. In the event that occurs, I will order a recess and reconvene.

And I normally, as chairman, wait until other members have asked their questions. And being that there is only one, I am at this point going to yield to the ranking member, Mr. Raskin, for questions.

Mr. RASKIN. Mr. Chairman, you're a true gentleman. Thank you very much for doing that.

Mr. Reese, let me start with you. I was very interested in your testimony. And thanks for coming all the way from Oklahoma. One of the things that cheered me about it was that you were not engaged in any kind of broadbrush attack on regulation. You were giving very specific examples of conflicts that just make your life difficult.

The specific example that you raised in your testimony, or at least your written testimony, was if you're handling sensitive data in the State, like Social Security data, IRS data, how many unsuccessful attempts of somebody trying to get into the computer must there be before you're required to shut it down and to close people out?

And you sort of set up a little graph where you showed that the IRS requirement was, if there are three attempts, I think the one from DOJ was perhaps no more than five attempts, and the Social Security agency was a recommendation of no less than three, no more than five. Okay.

And I did the little SAT question analysis and figured, okay, well, you could just set it at three. You would meet the IRS. You would also meet Department of Justice, because it would be not more than five. And the third one was just a recommendation. So it's not that big a deal.

On the other hand, why should it be so difficult for the Federal Government on something like that to come up with one governing principle? And I wonder if you've attempted to get the relevant agencies to come around on one coordinated, harmonized approach on that.

Mr. REESE. Thank you, Ranking Member Raskin, for your question.

So absolutely that is our goal. Our goal is seeking that partnership with our Federal partners. And, again, as a State agency, I absolutely view our Federal agencies as partners. We are all trying to do the same thing, and that is best use our citizen tax dollars to serve the needs of the citizens.

And so our goal in making sure that we are being fiscally responsible is where we get into challenges like this where we've got multiple different regulations that are imposed upon us and trying to find, in some cases, the most restrictive that applies. And, of course, in the example we talk about IRS and SSA and FBI.

Mr. RASKIN. Did you do anything to see if they would coordinate or harmonize?

Mr. REESE. So working through NASCIO, our national association, we have significant outreach where we come together and

have had several opportunities now to come together with the SSA and the FBI and the IRS who come speak to us.

In fact, our last meeting that we had here in Washington at the Hall of States, I believe we actually had in excess of, I think, 40 CIOs from other States that participated, if not all.

And those entities came and they spoke to us. And we actually get to talk about it. And they're there to answer our questions.

And so there's outreach. There's ongoing opportunities. But in typical State and government fashion, it's slow going. We're seeking support to continue those actions.

Mr. RASKIN. Gotcha.

Let me quickly come to you, Mr. Feeney. You mentioned NIST, which is actually in my district, so that piqued my curiosity, and I was thinking like an example that Mr. Reese gave.

Does NIST or can NIST play a role in just harmonizing and reconciling these things? It doesn't strike me as a really big deal except that we've got a big country with a lot of States, we have a lot of Federal agencies, and somebody needs to pull it together. But does NIST play that function?

Mr. FEENEY. NIST doesn't play that function exactly. But we coordinate and partner with NIST quite actively. So we took the NIST framework, which was a standard that had multi-stakeholder input, and we actually designed it specifically for the financial industry with NIST's both endorsement. And also NIST held two large conferences for us with the industry, with regulators and member firms, to really help develop that.

So they've been supportive of the work we're doing. They actually like it. They'd like to use it as a model for some other industries. And we are actively working with them.

We added two components to the NIST framework, because we thought they were very important to surface actively. One is governance and the second is third-party or dependency management. So we also have taken the NIST framework and extended it for the attributes of our industry, so we're working very collaboratively with them.

Mr. RASKIN. Thank you much.

Mr. Weissman, let me come to you. There have been some good points raised on specific issues like this on the need for harmonization and reconciliation of different Federal mandates for the States.

How can we distinguish those kinds of criticisms or points from a broadbrush attack on regulation itself and the system of rulemaking?

Mr. WEISSMAN. Well, I think, as you're pointing out, these are pretty particular issues. And it's not obvious that they broadly say anything about the administrative state.

I think in the cyber area the big problem is that there is no overarching legal framework. And although the executive could come up with one, Congress has actually failed on this.

We do have a crying need for, as Mr. Feeney was saying, really for an overarching cyber protection framework as well as a privacy protection one.

I agree with much of what he said. I disagree with his idea that we should preempt State law. I think it would be very important

to protect overall for States in this. But there does need to be a unified approach on that.

Beyond that, I'm not sure there is a massive problem of coordination. There may be issues in particular sectors. In many cases, the downside of lack of coordination is insufficient regulation rather than too much regulation.

Mr. RASKIN. Thank you.

I yield back, Mr. Chairman.

Mr. PALMER. I thank the gentleman.

I now recognize myself for questions.

Mr. Reese, how does having to comply with disparate Federal regulations impact the States? What kind of burden does that impose on the States?

Mr. REESE. So as you can imagine, in most areas of State government we have to be very cautious with the money that we have and how we spend it and what we do with it. And the challenge that we have is with these resources that we have to dedicate to compliance and in cybersecurity.

We're finding that we're having to put, as someone else here, I believe, pointed out, we know that about 40 percent of our resources within our compliance in cybersecurity are being utilized to our Federal compliance where, again, we're all for Federal compliance. We absolutely want to be following the laws because we need structure.

But our challenge is, is that we're having to spend so much time and so much duplicative time because of the multiple audits, again, when we're having the same audits over and over again.

And the fact that there's some differences that we have to go out and try to map as we had showed before, we've got to determine what the least common denominator is across those, the time constraints are just enormous. The amount of time that we spend, the thousands of hours we know.

We spoke with some of our other States, and we were able to log that in a single year Oklahoma spent over 10,000 hours in regulatory compliance, Maine spent over 11,000 hours, and Kansas over 14,000 hours just in our compliance and audits. Colorado itself had nearly 3,000 hours.

And so all of that is time and resources. And those resources, especially in days like we have today with cybersecurity being really a number one challenge for all of us, we'd rather be spending our time and efforts updating legacy systems and trying to enhance our security posture rather than trying to meet some of these, in many cases, outdated regulatory compliances.

Mr. PALMER. I ran a State-based think tank for 24 years and worked very closely with State legislators and administration official across, I think, four or five governors. And I am very aware of the cost imposed on the States and the inefficiencies from duplicate regulations, obsolete regulations, extremely overly complex regulations. It wasn't that the States weren't interested in complying. It was in many cases they didn't know what complying meant. And we spent an enormous amount of money.

Mr. Riggi, it's interesting, in your testimony you talk about what's going on in healthcare and how the patient-physician relationship is impacted by overregulation. One example, that would be

ICD 10, where basically you've got doctors that are compromising time with patients—or their time with patients is compromised because now they've become data entry people.

Would you like to comment on that?

Mr. RIGGI. Well, again—well, first, I'd just also like to clarify for the record that the AHA does understand the necessity of regulations to provide safety and high quality care for patients.

Again, the implementation of ICD 10 does require a significant amount of physician time. And I think for us to make sure we give you the most accurate response, it would be better for me to provide you a written response on that one, sir.

Mr. PALMER. That would be fine with me.

I introduced a bill to postpone the implementation of ICD 10 primarily because I grew up in a rural area. I grew up dirt poor basically in a house that had cardboard between the two by fours. And at the time I grew up, we did have a little doctor in a town that didn't even have traffic light.

You won't find that anymore. And one of things that I saw happening with ICD 10 was—and even made rural healthcare even harder to provide, literally, doctors were selling their practices or they were just flat out retiring, shutting the door.

And that's an example of how overregulating can have a very negative impact, particularly in these rural healthcare settings where they're already undercapitalized. It's also impacted wait times, and like I said, the amount of time that a doctor's able to spend with a patient.

And if you want to see what overregulation of a healthcare system looks like, take a look at Canada. The Fraser Institute published a report, the Huffington Post commented on this, that showed that between 1993 and 2009 there were between 25,000 and 63,000 women died on waiting lists waiting for treatment. The wait times have increased that much.

They just called votes. I'm going to go ahead and ask a couple other questions here before we recess.

But I want to go back to Mr. Reese and ask you, how do the Federal regulations keep pace with the evolving technology in the business models across State governments.

Mr. REESE. They do not.

Mr. PALMER. That is what I thought you'd say.

Mr. REESE. Our challenge is we find ourselves in a lot of cases when we're dealing with our regulatory compliance, we're actually dealing with third-party auditors. And the third-party auditors are coming in and doing different audits, getting different results on the same regulations, on the same systems.

And the technologies that they're auditing us on are not consistent. Their understanding of the technologies are not consistent with the technologies that we're using today. And in some cases, they're limiting our ability to use what we believe would be more cost-effective, efficient, and possibly even more secure technologies because we can't check the box with the auditor. So we have to go back and spend more money, using older technologies, costing the State more dollars, than if we could actually make good business decisions.

And a lot of this has to do with that those Federal regulations need to be able to keep up. We need to figure out how we can harmonize and be involved in those discussions and decisions, and how we can do it quicker so that we can keep up with the evolving technology.

But your point is absolutely spot on.

Mr. PALMER. What I found, again, working with the think tank, is that the people who are responsible for regulating are not people who are trying to mess things up. They're trying to do a good job. But they're as frustrated as everybody else because you call one regulator and get an answer, and 2 or 3 weeks later you call another regulator and you get a different answer. And it's frustrating them, because they want to do a good job.

Mr. Feeney, I'm going to ask this question, then we're going to take a recess to go vote. How much does it cost the financial institutions to apply with disparate regulations? And I'm interested in this because this additional cost gets passed on to the consumers, and I think it has a disproportionate impact on older customers and lower-income customers.

Mr. FEENEY. Right. So I can't speak to the specific aspect of that. I can tell you in 2016 the industry spent $9.5 billion on regulation, $1.5 billion of that was spent by the largest firms.

Mr. PALMER. Wait a minute. Wait a minute. According to the report that Mr. Raskin said came from OMB, I think you said that the regulatory cost was only $5 billion, but you say the regulatory cost on the financial institution was $9 billion?

Mr. FEENEY. I think quite a bit in the industry, across the industry, and that was a single-year review.

Mr. PALMER. Thank you.

Mr. FEENEY. The challenge is more, and I think Mr. Reese had referenced it, is that our industry, they are trying to keep up with the changes in technology, but you can't. It's just too fast paced, too hard.

We were able to use that sector profile, for instance, and take the question set down to about 400 from thousands. And what that does is provide you some latitude in simplifying the diagnostic statements that auditors or examiners would use. And there are ways to actually apply these types of tools to help the regulators, help the industries, I say that plurally, to really minimize the cost. And I think there are a number of things we can do in that arena.

Mr. PALMER. Okay. Hold on. I'm going to suspend for just a minute.

Mr. RASKIN. Mr. Chairman, with your permission, I'd like to submit for the record the OMB report from which I drew the figure, about $4.9 billion. Thanks.

Mr. PALMER. Okay. This is going to be a long vote series, so in consultation with the ranking member, what I'm going to do is I'm just going to make a couple other points here. Any additional questions will be submitted in writing. Because one thing that the ranking member and I do have a constitutional responsibility to do, and that is vote, and a political responsibility as well.

I do want to make some points that were in the OMB report, and these are quotes from the report, that it was a perspective analysis that they say may overestimate or underestimate both benefits and

costs. Retrospective analysis can be important as a collective mechanism. And that this was not an actual analysis of actual cost and benefits and that it only applied to about 1.6 percent of all the regulations.

So I tend to be somewhat dismissive of the OMB report, because my experience, again, working with the think tanks and being focused on trying to come up with sensible regulations. This idea that those of us on the Republican side of the aisle are for getting rid of all the regulations is just political nonsense. What we want are sensible regulations.

Regulations have improved the quality of life in our country. They've protected consumers. They've in some respects protected the relationship between the State and Federal Government.

What we want to do is get rid of the obsolete, the duplications, and the contradictions, and get it down to regulations that businesses can comply with, that they understand.

And one of the reasons that this is important is that in I think it was 2014—2015—the Gallup organization put out a report entitled basically—I think that the working title was "Is Entrepreneurism Dead in America?"

Prior to 2008, according to the Gallup study, there were 100,000 more businesses that started up than closed. But by 2014, there was 70,000 more businesses closed than started up. And according to the report, the primary reason for that was regulations.

I've tried to point out to people that businesses are not anti-regulation. They're anti-uncertainty. They're anti-complexity. And what we want to try to do in working to reform regulations is as much as possible reduce the uncertainty and the complexity, so that some person who has some capital to invest can make a sensible investment, whether it's starting a business or expanding a business or hiring more people.

With that, if there are no further questions—let me find my script.

Okay. The ranking member would like to make a closing comment. I yield to him.

Mr. RASKIN. Mr. Chairman, thank you very much.

And I want to just start my closing statement by saying how much I agreed with what you just said, that we're not opposed to rules which have, indeed, advanced the public interest, but obsolete rules or duplicate rules or contradictory rules, and I think we can all agree to that.

You know, nobody is in love with regulation, and the biggest tax is on people's time. And that might be one thing for big businesses, which often support a lot of regulation, but for small businesses it's very tough.

But I think about the 2010 BP oil spill, which was one of the worst environmental catastrophes in our history, which caused 11 deaths, immediately the deaths of more than a million coastal seabirds and other animals, and 5 million barrels of oil poisoning the whole Gulf of Mexico ecosystem.

That was a failure of regulatory enforcement just like the same year the collapse of the coal mines in Mexico, which led to dozens of deaths and a real calamity in that country.

So we need regulation. We need strong regulation. But I agree with you, we should be doing whatever we can to get rid of the duplicative, unnecessary, and obsolete regulation.

I yield back, Mr. Chairman.

Mr. PALMER. I thank the gentleman.

I thank our witnesses again for appearing before us today.

The hearing record will remain open for 2 weeks for any member to submit a written opening statement or questions for the record.

If there is no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 3:08 p.m., the subcommittee was adjourned.]