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.

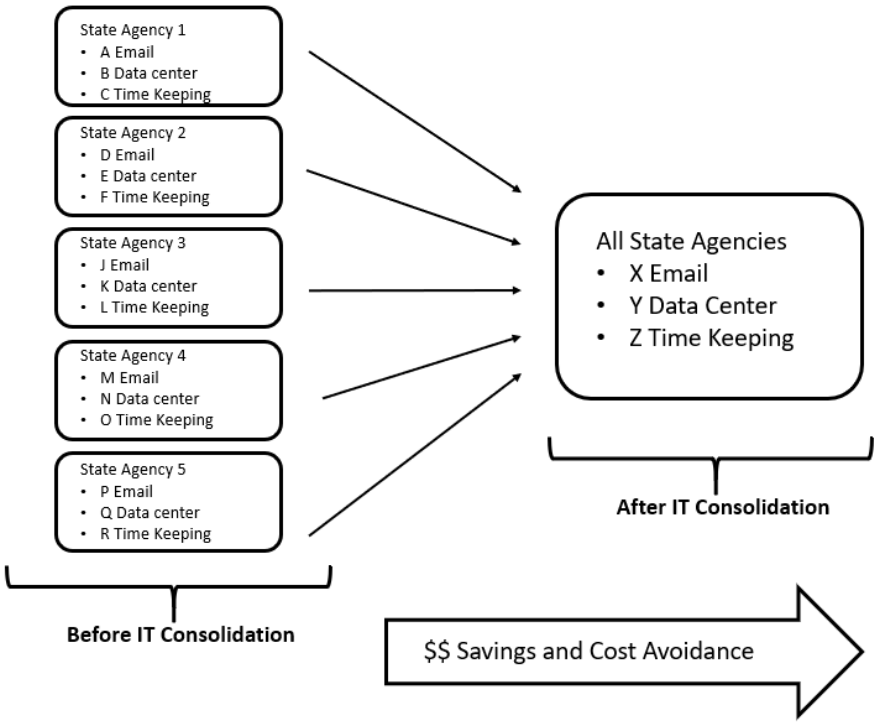


Figure 1: Graphic representation of IT Consolidation/Unification

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)

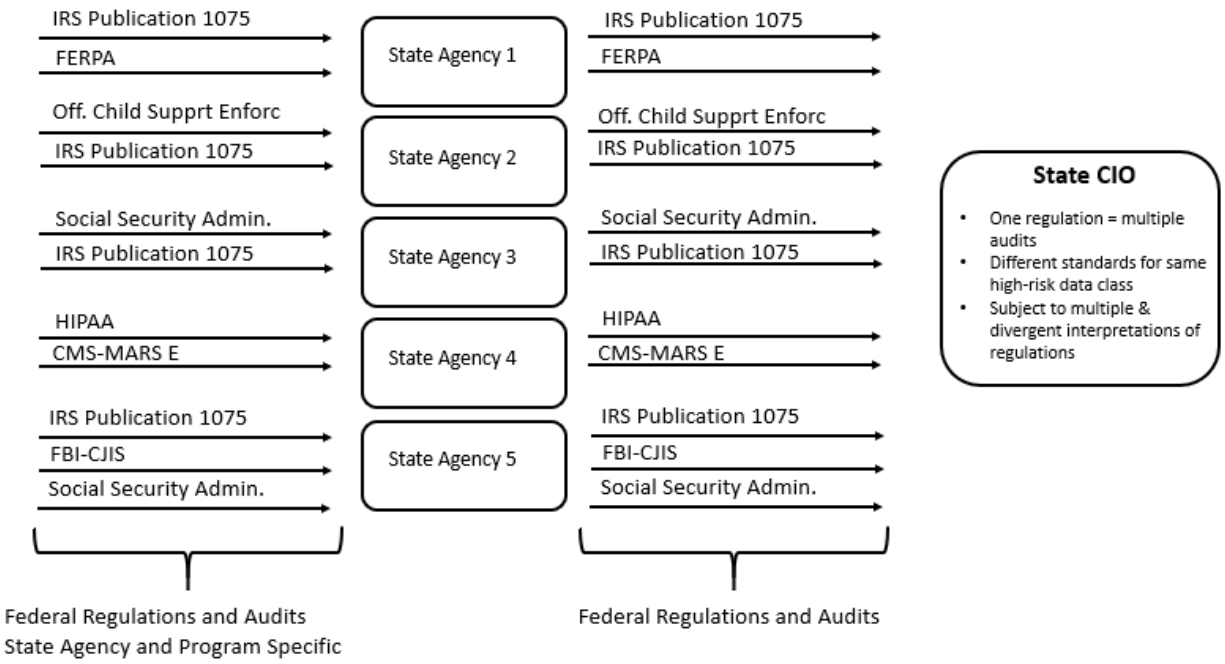


Figure 2: Current state of federal regulatory impact on state CIOs

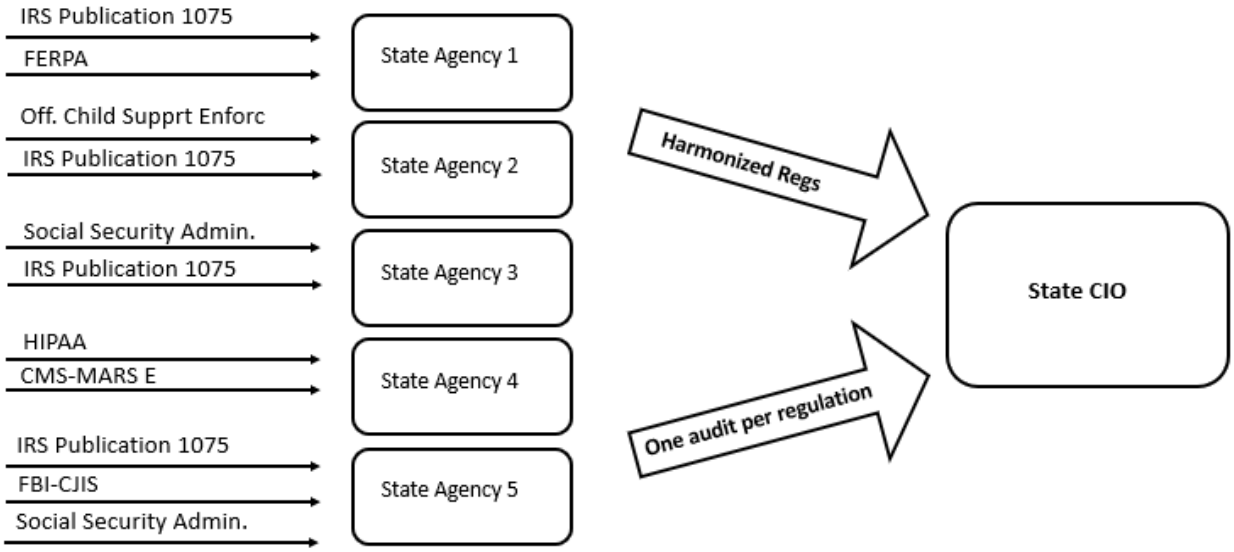


Figure 3: Desired state of federal regulatory compliance and audits

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.

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.

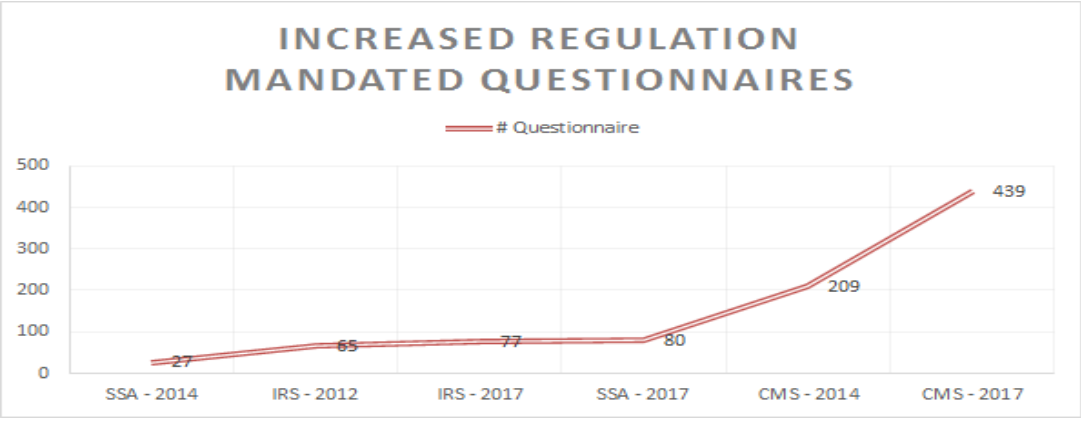
1. The State must analyze over 1,000 pages of Federal audit questionnaire.
2. The single source document for almost all the questions/mandates is the National Institute of Standards and Technology (NIST) Security Controls.

#	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