Statement before the Senate Homeland Security and Governmental Affairs Committee

"Cybersecurity Regulation Harmonization"

Testimony of James "Bo" Reese

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

June 21, 2017

Chairman Johnson, Ranking Member McCaskill, and members of the committee, thank you for inviting me to testify before you today on federal data security regulations and their impact to state governments.

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 vice president of the National Association of State Chief Information Officers (NASCIO).

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 chief information officers (CIOs) are governor-appointed, executive branch officials who serve as business leaders and advisors of information technology 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 and others are executive directors; regardless of the title, state CIOs share the common function of setting and implementing a state's IT policy.

Today, I would like to provide the committee an overview of how federal data security regulations impact our work to introduce efficiencies and generate savings for state taxpayers. 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.

IT Consolidation/Optimization Produces Efficiencies and Savings for Taxpayers

As the technology solutions provider for state executive branch agencies, state CIOs aim to operate IT infrastructure as if state government were one, unified enterprise. In doing so, state CIOs seek to maximize efficiency and leverage economies of scale where possible; this results in savings for state government and ultimately the taxpayer. Because of these known benefits, IT consolidation/optimization remains a top priority for state CIOs across the country. Indeed, every year for the past ten years, IT consolidation/optimization has appeared in the top three on the annual NASCIO Top Ten Priority list.

Regarding the IT consolidation effort in my state, the Oklahoma Legislature passed the Oklahoma Information Services Act[1] in 2009, which created the position of chief information officer. It also mandated an assessment of technology and telecommunications assets and services. The 2009 study found:

- An inability to leverage buying power across state government.
- The over-provisioning of IT infrastructure and human capital resources as each agency incorporated its surge capacity into its design and procurement.
- Expensive integration requirements to share data across agencies.

[1] https://legiscan.com/OK/text/HB1170/2010

- Significant risks due to a lack of maturity in basic processes including, backup, fault tolerance and disaster recovery.

The assessment's findings accurately reflected the pre-consolidated IT environment during which the state was supporting 76 financial systems, 22 unique time and attendance systems, 17 different imaging systems, 48 reporting and analytics applications, and 30 data center locations. To address these inefficiencies, the Oklahoma Legislature passed and the governor signed the Information Technology Consolidation and Coordination Act of 2011, which charged the Oklahoma Office of Management and Enterprise Services (OMES) with increasing the effectiveness and efficiency of the state's technology services. The law's legislative intent was to:

- Reform and consolidate the IT structure, operations and purchasing procedures of the state to ensure that state government promotes and encourages private sector growth in a competitive global economy;
- Move state government forward with respect to electronic purchasing, billing and payment services, and other transactions, to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers;
- Streamline and consolidate systems for financial and administrative services, with particular emphasis on combining the 76 financial systems, 22 unique employee time and record-keeping systems, 17 types of document imaging systems, 30 data center locations and 129 electronic mail and smart phone services used by the state; and
- Coordinate and require central approval of state agency IT purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies.

Over the past five years, OMES has reduced redundancies, made large strides to unifying technology, and completed consolidation of the 72 of the 78 mandated[2] state agencies and more than 30 voluntary agencies. Consolidation has resulted in $283 million of estimated reduced spending and projected savings. To complete the legislative mandate, OMES Information Services will consolidate the remaining mandated agencies by the end of FY 2017. <u>While we are well on our way to achieving the goals set by our legislature, one of the biggest hurdles in achieving this vision has been compliance with federal data security regulations.</u>

STATE CIOS MUST COMPLY WITH VOLUMINOUS FEDERAL DATA SECURITY REGULATIONS

I have described how we have approached consolidation/optimization in Oklahoma and would also like to give you the national perspective. As previously mentioned, state CIOs aim to operate the state government IT environment as a unified, single entity or "enterprise." The efficiencies and financial savings achieved by streamlining or consolidating the state's IT

[2] A "mandated" agency can be understood as a state agency that receives appropriations from the state. "Voluntary" agencies are those that are self-funded and do not receive state appropriations such as various boards and commissions.

environment are obfuscated by complex, disjointed, federal data security regulations that were issued in a de-centralized and "siloed" fashion.

State CIOs support the mission of state agencies and the federal programs they administer with 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 or receive federal funds or grants, state CIOs and the larger IT enterprise must also comply with and abide by federal data security regulations that are imposed on those state agencies. Thus, state CIOs find themselves operating in an increasingly complex regulatory environment driven by disjointed federal regulations. Below are some of the federal data security regulations with which state executive branch 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[3]
- 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)
- Gramm Leach Bliley Act
- Child Internet Protection Act of 2000
- Child Online Privacy Protection Rule of 2000

In addition to various federal regulations, state CIOs are also pushed to adopt other standards and frameworks that contracts and federal grants necessitate:

- NIST and FIPS standards (e.g. NIST 800-53 Revision 4)
- NIST Cybersecurity Framework
- NIST Risk Management Framework
- SANS and CIS Top 20 Controls
- Federal Information Security Management Act[4]
- Control Objectives for Information and Related Technologies (COBIT)
- ISO/ISE 27000 Series
- Payment Card Industry Data Security Standard (PCI-DSS)

[3] 45 CFR §307.5 Mandatory computerized support enforcement systems.

[4] FISMA applies to federal agencies and "organizations operating 'on behalf of' federal agencies. Determining whether FISMA applies to state agencies is complicated and while OMB has issued guidance clarifying FISMA's scope, which could include state governments, OMB guidance is unclear on when potential entities are acting "on behalf of an agency" and thus subject to FISMA. Many state CIOs comply in an abundance of caution.

While compliance with these regulations can be onerous, state governments and state CIOs understand, appreciate, and share the goal to which these regulations strive: protecting citizen data. From the cradle to the grave, state governments record, retain, and secure data related to all aspects of an individual's life; birth and death certificates, driver's licenses, voting registrations, professional licensing, health data, prison records – these are just some of the everyday data points that state governments must record, retain, *and* protect.

State CIOs invest an inordinate amount of time identifying duplicative regulatory mandates or their differences, participating in federal audits, and responding to inconsistent audit findings. These challenges in and of themselves are not unmanageable; the real issue is that they can and have impeded efforts of state CIOs to introduce efficiencies and generate savings for taxpayers.

REGULATORY SIMILARITIES ARE NOT RECOGNIZED IN THE FEDERAL DATA SECURITY AUDIT PROCESS AND RESULT IN DUPLICATIVE OR INCONSISTENT COMPLIANCE EFFORTS

Many federal data security regulations are similar in organization and substance; data security regulations generally address five common categories: physical safeguards, access controls, awareness and training, disaster recovery, and technical network and system requirements. Federal data security regulations are also similar in that the information that they seek to protect is usually varying levels of "high-risk" data such as federal tax information or health information. However, while data security regulations may share similarities, the federal audit process does not recognize regulatory similarities and puts the state CIO in the position of responding to the same compliance questions for multiple federal auditing entities. This results in an inefficient use of scant state personnel and financial resources.

To illustrate the issue of duplicative audits – in Oklahoma, the IRS audited one state agency twice because it viewed two programmatic elements of the agency as separate entities. My office had to answer questions, attend meetings, and deliver additional explanatory material twice for one state agency because it was seen as two by IRS auditors. Additionally, the audit findings were inconsistent; one audit team had a finding and the other did not, despite only one IT environment being the subject of both audits.

For more illustrations and perspectives from state chief information security officers (CISO) on the federal data security audit processes, please see the attachment.

REGULATORY CONFLICT HINDERS REALIZATION OF IT CONSOLIDATION/OPTIMIZATION BENEFITS

Complicating matters, differences in regulatory policy or regulatory conflict can also impact IT consolidation/optimization efforts negatively. As previously mentioned, federal data security regulations typically address cybersecurity in five common fronts and again, the substance of regulatory mandates can be quite similar. Because of existing overlap and similarities among the different federal data security regulations, even a seemingly minor difference can obscure the goal of IT consolidation/optimization which aims to streamline IT applications and simplify the enterprise IT environment to produce savings for taxpayers.

One example of regulatory conflict is reflected in different standards regarding breach or incident notification. The IRS requires incident notification within 24 hours[5] and the Centers for Medicare and Medicaid Services (CMS) requires notification of a breach "without unreasonable delay."[6] Both tax information and health information are considered high-risk data points and should be treated similarly, again, based on the level of risk and not compliance requirements.

Another example of regulatory conflict involves session lock out, or the time that a computer will block access after periods of inactivity. IRS Publication 1075 requires that session lock out occur after 15 minutes of inactivity; FBI-CJIS regulations require session lock out at 30 minutes. While a 15-minute difference may seem insignificant to the casual observer, in practice this means that the state CIO must configure the enterprise IT environment two different ways for data of similar risk. These kinds of regulatory conflicts introduce unnecessary complexity to state IT and hampers IT consolidation efforts.

INCONSISTENT FEDERAL AUDITS DRIVE STATE CYBERSECURITY INVESTMENTS BASED ON COMPLIANCE AND NOT RISK WHICH RESULTS IN A LESS SECURE POSTURE

When federal data security audits are conducted and produce "findings" of a critical nature, state CIOs must direct their attention and resources to remediating and addressing those "findings" to satisfy federal auditors and avoid any potential negative impact to citizens. This approach is problematic for state government cybersecurity because it encourages state CIOs to make check-the-box compliance investments instead of ones based on *risk*, which is the more secure approach[7] to managing sensitive data.

As states plan for IT consolidation, they will phase out old, less secure technology and schedule their replacement, as IT consolidation is usually a multi-year process. A federal data security audit can be very disruptive to IT consolidation because audit findings of a critical nature must be addressed within a very short period of time that may not align with the state's IT consolidation schedule. Put another way, federal data security auditors can impose their view of the state's risk without the ability to consider the state's comprehensive enterprise risk assessment or schedule for system upgrades.

STATE CIOS STAND READY TO WORK WITH OUR FEDERAL PARTNERS TO HARMONIZE REGULATORY POLICIES AND NORMALIZE THE AUDIT PROCESS

Like our federal partners, state CIOs are acutely aware of the risk inherent in sharing sensitive data. Likewise, we appreciate efforts by the federal government to secure and protect sensitive citizen information because we also share that responsibility at the state level. But, we must accomplish our shared goal without overly burdening state governments, ensuring that we are

[5] https://www.irs.gov/uac/reporting-improper-inspections-or-disclosures

[6] https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/Privacy_Data_Breach.html

[7] "A comprehensive risk management approach provides the ability to identify, assess, respond to, and monitor cybersecurity-related risks and provide organizations with the information to make ongoing risk-based decisions." NIST Cybersecurity Framework, page 3.

delivering government services to citizens in the most efficient and cost-effective manner. In recognition of that shared mission and responsibility, we want to work with our federal government partners to harmonize disparate regulatory requirements and normalize the audit process.

On behalf of our nation's state CIOs, I want to thank the Committee for addressing this issue and inviting NASCIO to share our perspective with you.

Thank you for your time and attention. I look forward to answering your questions.

Attachment

Statements Regarding and Examples of Inconsistent Federal Data Security Regulation and Audit Practices

ARKANSAS

The IRS has onerous requirements that do not contemplate cost and lack a policy justification. The IRS decided that if someone is using a VoIP phone, any phone call containing a discussion of FTI must be recorded and kept for seven years. The storage requirements, alone for this, are huge.

With the recent change from functional audits to IT audits there has not been a corresponding change/upgrade in the technical expertise on the IRS' part. Usually, when addressing a finding, it involves a conference call with the IRS and their technical contractor. When questioned, the contractor does not want to disagree with the IRS, so the state is left with little actual guidance. This contributes to our problems with mitigation.

Frank Andrews, CISO, State of Arkansas

DELAWARE

Federal security regulation pain points include inflexibility from federal auditors. We scheduled a 5 day visit but went home early due to a snow storm forecast. We had a number of documents that were "internal review only" documents; not to be taken offsite. 2-3 months later, those federal auditors picked things up and asked for the internal documents to be emailed. We said no and offered 3 options; they asked again for the internal documents (sensitive) to be emailed. This issue is still unresolved.

Elayne Starkey, CISO, State of Delaware

ILLINOIS

In Illinois, we encounter multiple IRS audits that ask the same questions across five separate agencies. There is also a lack of consistency on certain controls such as encryption rules, password rests, and now background checks. FBI-CJIS has clear guidance and standards on the types of individuals/entities that that must obtain a background check and the access to which they are privileged but IRS Publication 1075 merely states that personnel that have access to federal tax information (FTI) must be fingerprinted but includes no guidance on standards.

The continuous cycle of auditors focusing on different regulations creates an extreme burden on the states. Since each auditing unit requires testing by auditors, weeks if not months of personnel hours are wasted simply repeating the same tasks for each audit event.

Kirk Lonbom, CISO, State of Illinois

COMMONWEALTH OF KENTUCKY

We have 3 agencies (Cabinet for Health and Family Services, Department of Juvenile Justice, and Department of Workforce Investment) that receive Social Security Administration (SSA) data and 4 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 7 unique need and use agreements. As such, we have 7 agency level audits for each need and use agreement and 1 additional specific to IT as the state transmission center (STC) for a total of 8 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 4 agencies for the IRS and 3 for the SSA. This is single source data from a common federal repository. Where 1 compliance review would suffice, I have to respond to 7. 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.

David Carter, CISO, Commonwealth of Kentucky

LOUISIANA

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 (right).

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

As you can see, consistency is lacking and the agencies were audited with the same exact federal regulation.

Dustin Glover, CISO, Louisiana

MAINE

Overview:

1. The complexity of regulatory audit, and the duplication of requirements and reporting from different regulators, represent thousands of hours of opportunity cost. For instance, the State of Maine spent over 2,500 hours on the Social Security Administration audit alone.
2. Redundancy between different regulatory reporting requirements is common, with many questions asking for the same information, but worded slightly differently. We calculate that over 50%of the questions cover the same topics: Cybersecurity, Disaster Recovery, Admin Rights Monitoring, Access Monitoring, etc.

3. The regulatory oversight spans across multiple Federal agencies. Simplifying and combining similar regulatory requirements will enable States to greatly reduce the hours spent addressing compliance.

Regulatory Impact & Burden:

The State of Maine regulatory landscape includes 6 Federal agencies.

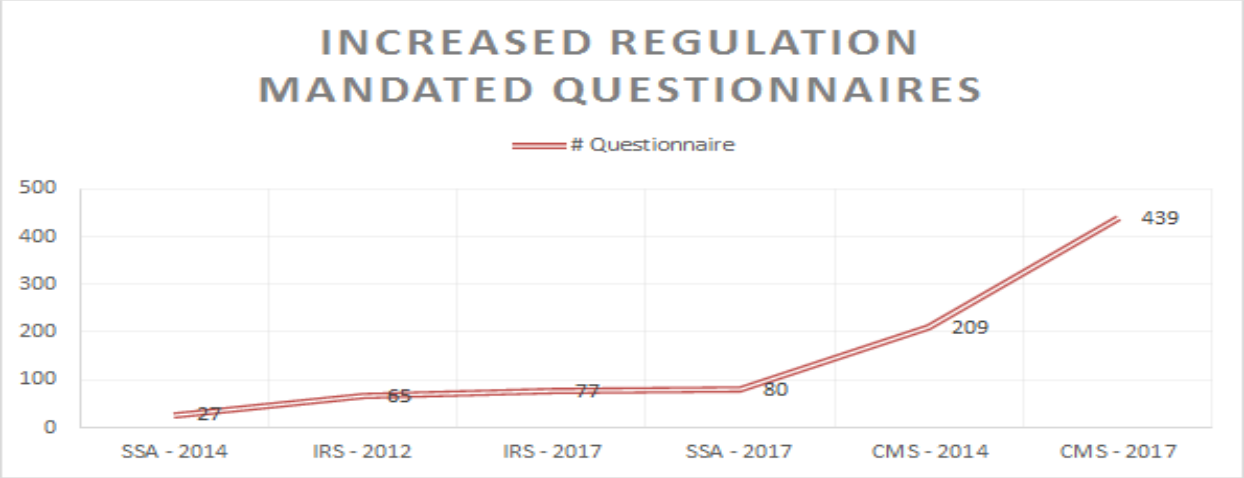
1. The State must analyze over 1,000 pages of Federal audit questionnaire.
2. The single source document for almost all the questions/mandates is the National Institute of Standards and Technology (NIST) Security Controls.

#	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	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

	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.	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.

Victor Chakravarty, Associate Chief Information Officer, Infrastructure, State of Maine

MONTANA

The State of Montana experiences roughly 9 federal audits every year; the audits cover IRS Publication 1075, Social Security Administration (SSA) requirements, and FBI-CJIS. They all have different requirements related to records retention, passwords, encryption, and physical security. Our largest pain point is the number of audits with different requirements and the need to address each one individually.

We have also experienced inconsistent audits as well as the inflexibility of mitigation efforts that clearly protect the data, but do not "check the box." One other item that is very frustrating is that when we are connecting with some Federal agencies like SSA, we request them to connect in a manner that meets their requirements i.e. through secured connectivity - VPN, but they cannot do it themselves because of cost, resource, or some other limitation.

It is very concerning to me how much money is being spent to complete all of these audits when one audit with consistent requirements could be completed for all Federal agencies.

Lynne Pizzini, CISO and Deputy CIO, State of Montana

NORTH CAROLINA

Issue 1: In addition to IRS engaging 3 different agencies in NC on differing schedules, the IRS findings, when remediated on the same infrastructure are not being closed out consistently. Recommend: Engage once, close once. Provide one Corrective Action Plan (CAP). Federal agencies should agree on the use of a Governance, risk management, and compliance (GRC)

solution to manage CAPs or Plan of Action and Milestones (POAMs); could be similar to U.S. Department of Defense's Enterprise Mission Assurance Support Service (eMASS).

Issue 2: Inconsistent approach to the implementation of security controls and acceptance of compensating controls implemented. Federal agencies tend to interpret their own definition of the controls which can increase cost for implementation. As a result, the North Carolina Department of Revenue (which is subject to IRS Publication 1075) has created a separate on premises email and other stand-alone solutions (as opposed to utilizing central IT services) to meet the "intent" of IRS 1075.

Recommend: Agencies that regulate any sensitive data type should adopt a common framework and add specific details on intended end result. Federal agencies should also review the changing landscape and update control requirements to be more adaptive.

Maria Thompson, CISO, State of North Carolina

WEST VIRGINIA

In my state, we have to spend scarce funding on services to map all federal regulations and requirements together to make them somewhat manageable. We spend valuable human capital and scarce funding to process multiple audits for the same federal regulation such as IRS Publication 1075. This creates complications in drafting and managing local security policy with zero flexibility. The federal approach is not based on risk management but rather "checkbox security" which forces the state to expend funds on low risk issues instead of a high-risk issue to maintain compliance.

I use human capital (i.e. Full Time Equivalents FTE) and scarce funding to manage multiple frameworks. If federal agencies were on the same page, those resources could be used more effectively to improve the state's security posture.

Also, consider FEDRAMP. It was designed so that vendors could provide cloud services with a trusted (3rd party) audit of the security. Why not use the same approach for the relationship between the states and federal agencies? One audit provides the mechanisms by which federal agencies have assurance in security and states have the flexibility to apply a risk management (as opposed to a compliance-based approach).

Josh Spence, CISO, State of West Virginia

WISCONSIN

Varying log retention requirements are difficult and costly to maintain. The worst is a 7-year audit trail retention requirement from the IRS. Realistically, what is the value of a 7-year-old log?

In addition to the cost of duplicative audits to the states, there would be a savings at the Federal level if they made one combined audit per State.

Bill Nash, CISO, State of Wisconsin